Review of security in VANETs and MANETs

Mai Abu Baqar
Faculty of Engineering
Al-Balqa' Applied University
Jordan
Mai_abubaqar@yahoo.com

Hamza Aldabbas
Prince Abdullah bin Ghazi faculty of Information and Technology.
Al-Balqa' Applied University
Jordan
aldabbas@bau.edu.jo

Tariq Alwadan
Faculty of Technology
The World Islamic Sciences and Education University
Jordan
Tariq.Alwadan@wise.edu.jo

Mai Alfawair
Prince Abdullah bin Ghazi faculty of Information and Technology.
Al-Balqa' Applied University
Jordan
may_alfa3ori@yahoo.com

Helge Janicke
Faculty of Technology
De Montfort University
UK
heljanic@dmu.ac.uk

ABSTRACT
Mobile ad hoc network (MANET) and Vehicular ad hoc network (VANET) are autonomous systems connected by wireless communication on a peer-to-peer basis. They are self-organized, self-configured and self-controlled infrastructure-less networks. These kinds of networks have the advantage of being able to be set-up and deployed anywhere and anytime because it has a simple infrastructure set-up and no central administration. Distributing information between these nodes over long ranges in such networks, however, is a very challenging task, since sharing information always has a risk attached to it especially when the information is confidential. The disclosure of such information to anyone else other than the

intended parties could be extremely damaging.

KEYWORDS
VANETs, MANETs,

1. INTRODUCTION

Recently, ad hoc networks received extensive attention in both industrial and military applications, because of the striking property of creating a network while moving from one place to another and not requiring any pre-designed infrastructure. This chapter therefore presents an introduction of mobile ad hoc networks (MANETs) in Section 2, with its characteristics described in Section 2.1: constrained resources, infrastructure less, low and variable bandwidth, dynamic topology, multi-hop communications, limited device security, limited physical security, and short range connectivity. These unique characteristics in MANETs present appreciable challenges, therefore Section 2.2 describes the vulnerabilities and challenges of MANET: lack of secure boundaries, restricted power supply, unreliability, lack of centralized management facility, threats from compromised nodes, and scalability.
There are many applications of MANETs therefore Section 2.3 presents these applications: home networks, enterprise networks, military applications, emergency response networks, sensor networks, and Vehicular ad hoc Networks (VANETs). Section 3 presents an introduction to VANETs, and describes the modern vehicles' components.
Section 3.1 presents history and background of VANETs by reviewing these projects and consortiums in VANET: PROMETHEUS project (program for European traffic with highest efficiency and unprecedented safety), DRIVE project (dedicated road drive infrastructure for vehicle safety in Europe), C2CCC (car2car communication consortium). Section 3.2 presents an overview of recent wireless communication technologies for VANETs: Wi-Fi, WiMAX and DSRC (Dedicated short range communication). Section 3.3 presents characteristics of VANETs: dynamic topology, random disconnection, mobility modelling, computational power, and variable density. The striking features of these networks raise both challenges and opportunities in achieving security, Section 4 presents these challenges.

Section 5 presents the security requirements: authentication, authorisation, access control, privacy, confidentiality, availability, survivability, data integrity, and non-repudiation. Section 6 presents both types of attacks: passive attacks are hard to detect because they are based on 'snooping' on transmitted packets between entities, whereas in active attacks the attacker tries to change or destroy the data being transmitted within the network. External active attack and internal active attacks are also described in Section 6. Section 7 presents a set of security mechanisms which can be used to enforce the security requirement: cryptography, digital signature, access control, authentication, traffic padding, notarization, and routing control. Section 7.1 presents the access control models: Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Role-Based Access Control (RBAC).

Section 8 presents an overview of the cryptographic background to understand work already done on securing VANETs and MANETs. Two main types of cryptographic algorithms are used in cryptography: symmetric key algorithms presented in Section 8.1 in which sender and receiver both use the same key (secret key) for encryption and decryption, whereas in asymmetric key algorithms presented in Section 8.2, the sender and the receiver uses two different keys for encryption and decryption. Public Key Infrastructure (PKI), Digital signature, and Digital Certificate will also be discussed in detail in Sections 8.2 and 8.3 respectively.

Finally, Section 9 presents a critical review of the security issues in both MANETs and VANETs. It also provides a survey of existing solutions in the field of security to highlight a particular area, not been addressed up to now: controlling the information flow that allows the originator to control the

dissemination of data communicated between nodes. This is to ensure that data remains confidential not only during transmission but also after it has been communicated to another peer.

2. Mobile wireless ad hoc networks (MANETs)

Mobile ad hoc networks are autonomous systems which consist of a number of mobile nodes that communicate between themselves using wireless transmission. They are thus self-organized, self-configured and self-controlled infrastructure-less. This kind of network has the advantage of being able to be set up and deployed anywhere and anytime because it has a simple infrastructure setup and no central administration. Mobile ad hoc networks (MANETs) are case of wireless ad hoc networks, progressively more popular and successful in the marketplace of wireless technology.

These networks are particularly useful to those mobile users who need to communicate in situations where no fixed wired infrastructures are available. Obvious examples are the military or the emergency services: one clear situation might be a fire fighter who needs to connect to an ambulance. In such situations a collection of mobile nodes with wireless network interface can form a transitory network (Sarkar, Basavaraju & Puttamadappa 2007). Recently, ad hoc networks received extensive attention in both industrial and military applications, because of the striking property of creating a network while moving from one place to another and it does not require any pre designed infrastructure.

2.1. The Characteristics of MANET

A mobile ad hoc network (MANET) is an independent system of mobile nodes linked by wireless connections. These nodes are free to move arbitrarily; therefore, the topology of wireless networks change swiftly and in an unpredictable manner.

Generally, direct communication in MANETs is possible only between adjacent nodes. Thus, communication between distant nodes is established using multiple-hop. Since the locations may change dynamically, as a consequence the interconnections between the adjacent nodes may change continually. Each mobile node functions as both host and router, relaying data packets from one node to another. MANETs have many characteristics that make them distinguishable from other wireless and wired networks (Al-Jaroodi 2002, Murthy & Manoj 2004, Toh 2001, Chadha & Kant 2007, Carvalho 2008) which are in detail:

- **Constrained Resources:** Most MANET devices are small hand-held devices like personal digital assistants (PDAs), laptops and cell phones. These devices have limitations because of their restricted battery-capacity, small processing power and storage facilities. Energy consumption is an important criterion when designing the MANET.

- **Infrastructure-less (Autonomous):** MANETs are based on the teamwork between independent peer-to-peer nodes that communicate with each other. Without any pre-planned arrangement or base station, all nodes have the same role in the network. There are no pre-set roles like router, server or gateways for the nodes participating in the network.

- **Low and Variable Bandwidth:** Wireless links which connect the MANET nodes have much smaller bandwidth than wired links. The effects of interference, congestion and noise are more significant.

- **Dynamic Topology:** MANET nodes can move arbitrarily; thus the nodes can dynamically enter and leave the network, continually change their links and topologies. This leads to frequent changes in the routing information.

- **Multi-hop communications:** The communication in MANET between any two nodes is performed by numerous intermediary nodes whose functions are to relay data-packets from one point to another. Ad hoc networks require multi-hop communications, for example, in Figure 1, nodes A and D must engage the help of nodes B and C to relay data-packets between them in order to communicate.

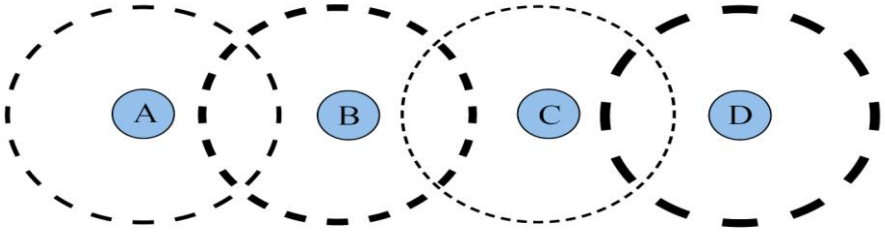


Figure 1: Mobile ad hoc network of four nodes, using the transmission range of nodes B and C in order to communicate between node A and node D

- **Limited Device Security:** MANETs devices are usually small and can be transported from one place to another. Unfortunately, as a result these devices can be easily lost, stolen or damaged.

- **Limited Physical Security:** MANETs are in general more vulnerable to physical layer's attacks than wired networks; the possibility of spoofing, eavesdropping, jamming and denial of service (DoS) attacks should be carefully considered. However the self-administration nature of MANET makes them more robust against single failure points.

- **Short Range Connectivity:** MANETs rely on radio frequency (RF) technology to connect, which is in general considered to be short range communication. For that reason, the nodes that want to communicate directly need to be in the close frequency range of each other.

2.2. The vulnerabilities and challenges of MANET

The key challenges in designing MANETs result from the decentralised nature and lack of central infrastructure like a base station, access point or server. In addition to that, all communications are carried out through the wireless medium. These unique characteristics present appreciable challenges for MANETs as mentioned in (Li & Joshi 2004, Papadimitratos & Haas 2003, Mishra & Nadkarni 2003, Zhang & Lee 2005):

- **Lack of Secure Boundaries:** In comparison with wired networks where the devices must have a physical access to the network medium, mobile ad hoc networks have no apparent secure boundary. There is no need for attackers to have physical access to the network; once the attackers are in the transmission range of any other devices, then they can join and communicate with other devices.

- **Restricted Power Supply:** In contrast to wired networks where the nodes can get their electrical supply directly from the power points, MANETs nodes are generally operated by small batteries

with limited lifetime. Nodes are therefore less likely to be able to operate intensive computations, which makes them vulnerable to a denial-of-service attack (DoS). This can be done by sending additional routing packets to a targeted node, in order to be executed by the targeted node in an attempt to exhaust its battery.

- **Unreliability:** Due to the limited battery supply and mobility in MANETs, the mobile devices cannot be assured as being reliable to serve communication participants; some nodes may behave in a 'selfish' manner when it finds that there is only limited power supply.

- **Lack of Centralized Management Facility:** The lack of centralized management makes the detection of attacks complicated. Mobile ad hoc networks are highly dynamic and large scale therefore they cannot be easily monitored. Also benign (non-malignant) failures in the mobile ad hoc network are fairly common, for example, transmission destructions and packet dropping. As a result, malicious failures will be more difficult to discover.

- **Threats from Compromised Nodes:** Due to the movement of the nodes in ad hoc networks, it can be challenging to detect the malicious attack carried out by a compromised node, particularly in a large scale ad hoc network.

- **Scalability:** In MANETs nodes entering and leaving the network cause frequent changes to the network topology; the network may consist of hundreds to thousands of nodes; the routing protocols configurations and key management services therefore have to be adjusted to fit these new conditions.

2.3. Applications of mobile ad hoc networks

There are many applications of mobile ad hoc networks; these have been listed in (Sarkar, Basavaraju & Puttamadappa 2007, Bharathidasan & Ponduru 2002, Murthy & Manoj 2004, Yousefi, Bastani & Fathy 2007, Carcelle, Dangand & Devic 2006, Yick, Mukherjee & Ghosal 2008):

1. **Home Network and Enterprise Network:** One use of MANET is in some home environments, such as home wireless networks, smart homes and personal area networks (PAN) which we can make communication between smart household appliances, in comparison with fixed wireless network, wireless ad hoc devices can move in free manner and they organise themselves in an arbitrary type. Roaming can be carried out while the devices are communicating with each other, which is suitable to businesses demand such as in office wireless networks, conferences, meeting rooms and networks at construction areas.

2. **Military Applications**: Mobile ad hoc network can be valuable to soldiers in order to establish communication for tactical campaigns; setting up a fixed infrastructure in enemy areas or in hostile lands may not be possible in such conditions. Whereas, MANETs can offer the required communication promptly and quickly. The coordination of military objects moving at high speeds, such as fleets of airplanes or warships is another application in this area.

3. **Emergency Response Network**: Mobile ad hoc network can be used to supply emergency management services applications, for example in disaster recovery, fire fighting, search and rescue operations where the whole communication infrastructure has been demolished or is unavailable. Deploying MANETs in these places can set up an infrastructure quickly.

4. **Sensor Network**: Wireless sensor networks can be deployed in ad hoc mode to assist monitoring and controlling physical surroundings from distant places with sufficient accuracy. These sensors might be equipped with a selection of components (processor, radio transceiver, actuator, micro-controller, and energy source) in order to measure several physical attributes like motion, temperature, moisture, atmospheric pressure, sound, vibration, pollution and velocity.
   Sensor networks are used in military applications such as battlefield observation; equipment ammunition; targeting; and nuclear, biological and chemical attack detection and reconnaissance. It is also commonly used in many manufacturing and civilian applications, such as monitoring product quality, controlling machines, healthcare applications, home automation control(smart home), and traffic control.

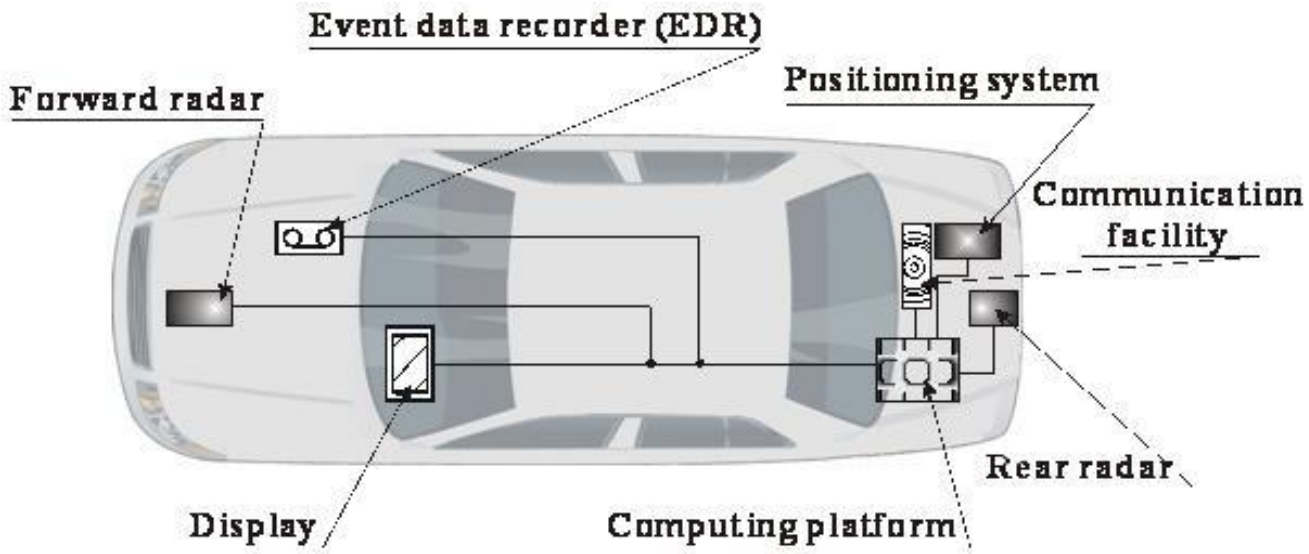
5. **Vehicular Ad hoc Network (VANET)**: It is a subclass of mobile ad hoc networks (MANETs), where the mobile nodes are vehicles; today vehicles are becoming "computer networks on wheels", these vehicles are free to move and organise themselves arbitrarily, which they can exchange information between themselves and Road Side Units (RSUs), in order to increase safety in the roads by warning the drivers about ongoing hazard situations, and increasing the responsiveness of their surroundings and make them more vigilant.

   In another aspect inter-vehicle communication(IVC) can be used to enhance passenger comfort and traffic system such as exchanging traffic information, weather information, petrol station, restaurants location and price information, and providing the interactive communication like offering access to the Internet.

3. Vehicular ad hoc networks (VANETs)

Vehicular ad hoc network is a new emerging network technology derived from ad hoc networks, which can provide wireless communication services between vehicles and adjacent road side units; it is a promising technology for future smart vehicle systems and intelligent transportation systems (ITS).

In VANETs, each vehicle in the system as in Figure 4 has a computing device, a short-range wireless interface, event data recorder (EDR), front and rear sensors and a GPS (Global Positioning System) device which is progressively more becoming common in vehicles today, in order to provide vehicles' location, speed, current time and direction.



(Olariu & Weigle 2009)
Figure 2: A modern vehicle is a network of sensors/actuators on wheels

3.1. History and background

The idea of inter vehicle communication (IVC) has gained considerable interest in the last few decades, which includes vehicle-to-vehicle (V2V), and vehicle-to-infrastructure (V2I) communications. In Europe for examples PROMETHEUS (program for European traffic with highest efficiency and unprecedented safety) project was created during 1987-1995 by eighteen European car manufacturers, incorporating more than forty research institutions in addition to state authorities; the main purpose of the PROMETHEUS project was automated driving (adaptive cruise control) for private cars. The next project DRIVE (dedicated road drive infrastructure for vehicle safety in Europe) was created during 1988-1994; the main purpose of the DRIVE project was to improve traffic efficiency and safety considering road-side infrastructure (Olariu & Weigle 2009). These projects led substantial progresses in European road transport; however the deployment of inter vehicle communication was not adequate enough to deploy, because of the need of a suitable wireless communication technology.

When new wireless technologies have emerged, to support the revolution of vehicular ad hoc networks, the number of academic and industrial interests in VANETs has increased. and many efforts moved from the pure research stage to the experimental and execution stage. As a result a non-profit organization called C2CCC (car2car communication consortium) was created by Audi, BMW, Daimler Chrysler, Fiat, Renault, and Volkswagen.

After that IEEE 802.11p task group was formed which is focused on providing wireless access technology for vehicular environment; in accordance with the official IEEE 802.11p working group project timelines, the standard is scheduled to be published in December 2010. Recently, Toyota and Microsoft have declared a 12 million dollar joint investment on including Microsoft's Azure cloud platform in upcoming Toyota vehicles for better telematics (Oates 2011).

The main goal of these projects and consortiums are to increase road safety, increasing transportation efficiency, and reducing the impact of transportation on the environment.

3.2. Wireless communication technologies for VANETs

In recent years various wireless network technologies have been developed to offer different services, increased coverage area and data rates. In this introduction we will describe in overview:

1. Wi-Fi

(abbreviation of Wireless Fidelity) is a class of wireless (LAN) devices; the technology is based on the IEEE 802.11 standards (Lehr & McKnight 2003). Today, Wi-Fi devices can be found in many desktop computers, smart phones, printers, and indeed all modern laptops and (PDAs) are equipped with Wi-Fi technology. Wi-Fi's original purpose was mobile computing devices (for example laptops in LANs), but is now progressively more used for more purposes, including VoIP phones, games, and televisions and DVD players. Wi-Fi today is more commonly used to provide an Internet LAN connection to Wi-Fi enabled devices like a computers, smart phones or PDAs. The above functions require the device to be within range of an access point.

The most common Wi-Fi standard IEEE 802.11g has a data transfer rate of around 54 Mbps; the range indoors is a maximum 150 feet (approximately 45 meters) and double that outdoors though, this depends on the conditions, like obstacles, power and weather. In Wi-Fi both 802.11b and 802.11g are using 2.4 GHz under the speed of 11 Mbps and 54 Mbps respectively, while 802.11n operates in both 2.4 and 5 GHz with theoretical speed 600 Mbps (Gast 2005).

In Wi-Fi MAC (Media Access Controller) users are competing when they are connected to Wi-Fi access point, and users therefore have different levels of bandwidth. Wi-Fi however is short range (tens of meters) can be encrypted with WEP(Wired Equivalent Privacy) or WPA and WPA2 (Wi-Fi Protected Access encryption).

2. WiMAX

(Worldwide Interoperability of Microwave Access) is based on the IEEE 802.16 standard (also called Broadband Wireless Access). WiMax was formed in 2001 by the WiMax Forum, in order to endorse WiMax as a standard (Andrews, Ghosh & Muhamed 2007).

WiMax was described as a standard based technology for use as "last mile" broadband delivery rather than using wires. WiMax was planned to be used to link Wi-Fi hotspots together. WiMax 802.16 operates at range of 10-66 GHz and is classified as fixed wireless broadband; later, in 2004 802.16a was updated and operates at lower frequency range 2-11 GHz and is classified as fixed wireless broadband as well; finally in 2005 mobile wireless broadband was created under 802.16 e which operates at frequency range of 2-6 GHz (Ghosh, Wolter, Andrews & Chen 2005).

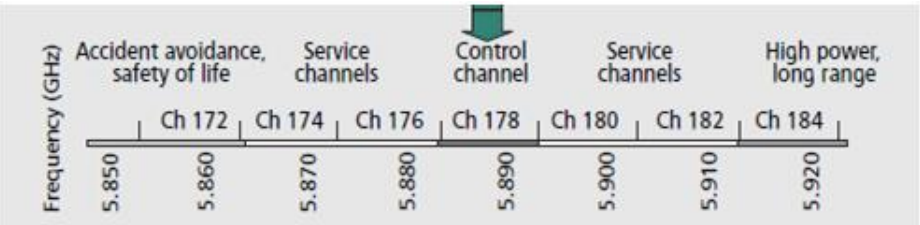
WiMax technology has an advantage which is not affected by obstacles like buildings. This makes WiMax especially useful and cost-effective for countryside homes where setting a traditional wire would be more difficult and very expensive.

WiMax is equipped with stronger encryption than Wi-Fi, and typically suffers less interference. WiMax speed in theory delivers up to 70 Mbps, and range coverage 112 Km. These numbers changes depends on the conditions, like obstacles, power and weather, expected values is 10 Mbps in 2 Km coverage area.

3. DSRC

In 1999, Dedicated Short-Range Communication (DSRC) spectrum was allocated by the U.S. Federal Communication Commission (FCC), for intra-vehicle communication at 5.9 GHz. The original goal was to make public safety applications possible in order to rescue lives and increase of quality of traffic flow (Biswas, Tatchikou & Dion 2006, Bai & Krishnan 2006), but it is now increasingly used for comfort applications. In order to decrease the cost and support DSRC development, they permitted the private services as well. DSRC supports vehicle speeds up to 120 mile/hour, and the transmission range is between 300m and up to 1000m. This will enable operations related to the improvement of traffic flow, highway safety, and other intelligent transport system (ITS) applications.

DSRC spectrum is divided into seven 10 MHz wide channels as shown in Figure 3, the Channel 178 (control channel) is confined to safety communications only. The two channels at the edges of the spectrum are kept back for future advanced accident avoidance applications and high-powered public safety usages. The four channels (service channels) are left for both safety and non safety usage (Jiang, Taliwal, Meier, Holfelder & Herrtwich 2006).



(Jiang, Taliwal, Meier, Holfelder & Herrtwich 2006)
Figure 3: DSRC channel arrangement

3.3. Characteristics of VANETs

VANETs have similarities with MANETs like low and variable bandwidth, short range connectivity, infrastructure-less, and self-organisation, but can be distinguished from MANETs by the unique characteristics such as high mobility and unreliable channels. These caused research challenges such as routing protocols, data broadcasting, and security issues. Most the routing protocols that have been used in MANETs cannot be applied in VANETs, because they suffered from poor performances caused by the fast movement in vehicles.

The most important differences between them is that vehicles in VANETs can move randomly but still predictably (restricted by geography of roads), even if they move at much higher speeds than traditional MANETs. Vehicles in VANETs are also have much higher power than in MANETs (Misra, Woungang & Misra 2009, Manui & Kakkasageri 2008, Olariu & Weigle 2009). At the end of this section a comparison between the characteristics of MANETs and VANETs is provided as shown in the Table 1.

- **High and Dynamic Topology**: Because of the high speed and random of movement in vehicles, the topology of VANETs changes rapidly (Li & Wang 2008), for instance, assuming that all vehicles have the same transmission range which is 300 meters, a link can be formed between any two vehicles if the distance between them is less than 300 meters. In the worst possible scenario, if there are two vehicles driving in opposite directions, with the speed of 60 miles/hour (26.6 meters/second) consequently, the connection will last only for at most 11.2 seconds.

- **Random disconnection (frequent fragmentation) in network scale**: The vehicles in VANETs are free to move; hence they can dynamically enter or leave the network. Consequently, the connectivity in VANETs would change frequently (Wisitpongphan, Bai, Mudalige & Tonguz 2007) which it will affect the network structure services, for example, in a low vehicles traffic density case, where there are two vehicles that need to communicate with each other, and there was only one vehicle in between them, if this vehicle changed its direction to another road, this will cause disconnection between these two vehicles, as well consider the obstacles (for example buildings, trees) that exist in the urban and crowded areas which they can prevent wireless signals, therefore the need to sustain the wireless connection must be improved by deploying more road side units or several relay nodes along the roads.

- **Mobility modelling and prediction**: Mobility and prediction model plays a significant role when designing protocols in VANETs, because of the high mobility of vehicles, high speed of vehicles and dynamic topology. Generally, we can predict the future position of vehicles if we know their speed and road maps, because the vehicles are restricted to pre-built high ways, roads, and streets (Fiore, Harri, Filali & Bonnet 2007).

- **High energy and computational power**: There are a common characteristic in VANETs which make them are distinguished from other networks; vehicles can have large energy, adequate storage, and high processor, powerful wireless transceivers and high data rate because nodes in VANETs are vehicles instead of small handheld devices as in MANETs.

- **Potentially large-scale and variable density**: In traditional wireless network the nodes number can be restricted or can be expected, in VANETs however the nodes number can be much larger and cannot be predicted, for example, assume an urban and crowded area with thousands of vehicles and a plenty of roads and streets, where the vehicles are located close to each other in the same area, and consider the case where vehicles are driving at period in the morning and evening of the greatest burden upon the channels of transportation in the same time (rush hour), in addition VANETs can be extended in large areas as far as the road is available. All these facts increase the large-scale probability in VANETs (Killat, Schmidt-Eisenlohr, Hartenstein, Rossel, Vortisch, Assenmacher & Busch 2007).

Characteristic	MANET	VANET
Constrained Resource	✓	×
Topology	Dynamic	More Dynamic than MANET
Mobility Prediction	×	✓
Multi-hop	✓	✓
Limited Device Security	✓	×
Limited Physical Security	✓	✓
Short Range Connectivity	✓	✓
Infrastructure less	✓	✓
Low and Variable Bandwidth	✓	✓

Table 1: Comparison between characteristics of MANETs and VANETs.

4. Security challenges for VANETs and MANETs

Since, security is an essential component in VANETs and MANETs, the striking features of these networks raise both challenges and opportunities in achieving security, unlike other traditional networks (wired) where nodes must have physical access to the network line or communicate through several lines of protection like firewalls and gateways. VANET and MANET use the wireless medium so attacks on a wireless network can come from all directions and target any node. It gives high opportunity to be attacked if does not has certain security measurements. Consequently, link attack ranging from passive attack to active attack, message replay, message leakage, message contamination and message distortion can occur. All these mean that VANETs and MANETs do not have a clear line of defence, and every node must be arranged for the different kind of attacks (Zhang & Lee 2005).

Therefore, in order to achieve high survivability and scalability, VANETs and MANETs should have a distributed architecture with no central administration, and of course the high mobility nature in these networks should be considered, since prior trust cannot be counted upon in such networks; any intended solution to the security aspects therefore, should be adaptive 'on the fly' to these changes and should have the ability to deal with large networks as in VANET it may consist of hundreds or even thousands of mobile nodes.

The distinctive characteristics of VANETs bring a new set of essential challenges to security design such as open peer-to-peer network architecture, sharing of the wireless medium, large-scale density, the high relevance of vehicle geographic location and dynamic network topology. These challenges noticeably make the looking for security solutions that perform both data protection and applicable network performance are required.

Distributing information between nodes in VANETs and MANETs over long ranges in such networks, however, is a very challenging task, since sharing information always has a risk attached to it especially when the information is confidential.

Normally in addressing network security, three significant issues need to be considered in the system: security requirements, security attacks and security mechanisms. Security requirements take account of the functionality required to provide a secure networking system, whereas the security attacks include the techniques that might be carried out to break these requirements. Finally, the security mechanisms are the fundamental elements used to enforce the security requirements. Section 5 therefore presents the security requirements: authentication, authorisation, access control, privacy, confidentiality, availability, survivability, data integrity, and non-repudiation. Section 7.1 presents the access control models: Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Role-Based Access Control (RBAC).

Attacks on VANETs and MANETs can be divided into two types: passive and active attacks. Section 6 therefore presents both types of attacks: passive attacks are hard to detect because they are based on 'snooping' on transmitted packets between entities, whereas in active attacks the attacker tries to change or destroy the data being transmitted within the network. External active attack and internal active attacks are also described in Section 6. Section 7 presents a set of security mechanisms which can be used to enforce the security requirement: cryptography, digital signature, access control, authentication, traffic padding, notarization, and routing control.

Section 8 presents an overview of the cryptographic background to understand work already done on securing VANETs and MANETs, as well as the recent research. Two main types of cryptographic algorithms are used in cryptography: symmetric key algorithms presented in Section 8.1 in which sender and receiver both use the same key (secret key) for encryption and decryption, whereas in asymmetric key

algorithms presented in Section 8.2, the sender and the receiver uses two different keys for encryption and decryption. Public Key Infrastructure (PKI), Digital signature, and Digital Certificate will also be discussed in detail in Sections 8.2 and 8.3 respectively.

Section 9 presents a critical review of the security issues in both MANETs and VANETs. It also provides a survey of existing solutions in the field to highlight a particular area, not been addressed up to now: controlling the information flow in these networks (Janicke, Sarrab & Aldabbas 2012, Aldabbas, Janicke, Abu Jassar & Alwada'n 2012, Aldabbas, Alwada'n, Janicke & Al-Bayatti 2012), aims to provide an architecture that allows the policy-based architecture to control the dissemination of data communicated between nodes. This is to ensure that data remains confidential not only during transmission but also after it has been communicated to another peer.

5. Security Requirements

The security requirements are specified by standards of several organisations such as the International Telecommunications Union (ITU-T), which defines the security requirement as a set of services provided by the system which ensures the adequate security level for data communication, by giving specific protection to system resources. ITU-T, in their recommendation X.800 and X.805 defines these requirements as follows (Al-Jaroodi 2002, Menezes, Van Oorschot & Vanstone 1997, Li & Joshi 2004, Stallings USA, 2005, Xing & Wang 2007):

- **Authentication**: Authentication verifies the identity of each node and its eligibility to access the network. This means that nodes in these networks are required to verify the identities of the communicated entities in the network, in order to ensure that they are communicating with the correct entity. This requirement is an essential and difficult requirement to satisfy. If the authentication stage was not fulfilled, no further requirements would be properly implemented. For example, if two entities are using symmetric-key encryption for securing the communication and one of these entities become compromised caused by the lack of authentication, then all encrypted material such as the shared key and the encryption algorithm will be available to that adversary entity.
- **Authorisation and Access Control**: Each node is required to have access to shared resources, services and personal information on the network. In addition, nodes should be capable of restricting each other from accessing their private information. There are many techniques that can be used for access control such as Discretionary Access Control (DAC), Mandatory Access Control (MAC) and Role Based Access Control (RBAC) (to be discussed in Section 7.1). Traditionally authorisation policies are related to auditing techniques to track resource usage and deduce statistics about nodes in the network.
- **Privacy and confidentiality**: Each node has to secure both the information that is exchanged between it and others, and secure the location information and the data stored on these nodes. Privacy means preventing the identity and the location of the node from being disclosed to any other entities, while confidentiality means keeping the secrecy of the exchanged data from being revealed to those who do not have permission to access it. Data confidentiality can be applied by using any encryption techniques based on secure key management system. Whereas protecting the users' privacy such as node-id, position, and travelling routes needs something more than encrypting the data, indeed sophisticated mechanisms are required to conceal those users' attributes such as using a pseudonym technique.
- **Availability and survivability**: The network services and applications should be accessible when needed, even in the presence of faults or malicious attack such as denial-of-service attack (DoS), while survivability means the capability of the network to restore its normal services under such these conditions. These two requirements should be supported in any network.

- **Data integrity**: The data transmitted between nodes should be received by the intended entities without been tampered with or changed by unauthorised modification. This requirement is essential especially in military, banking and aircraft control systems, where data modification would cause potential damage.
- **Non-repudiation**: This ensures that nodes when sending or receiving data-packets should not be able to deny their responsibilities of those actions. This requirement is essential especially when disputes are investigated to determine the entity which misbehaved. Digital signature techniques are used to achieve this requirement to prove that the message was received from or sent by the alleged node.

6. Security Attacks

Attacks on VANETs can be divided into two types, namely, passive and active attacks (Stallings USA, 2005, Murthy & Manoj 2004). Passive attack are based on 'snooping' upon transmitted packets between entities; the goal of the attacker is to acquire data that is being sent without modifying it, but not to stop the operation of the network, thus breaching the confidentiality requirement. Passive attacks are hard to detect because the data packets are sent and received normally and neither the sender nor receiver is aware that the attacker has read the packet or has intercepted the traffic pattern. Therefore, it is more important to prevent such this attack rather than to detect it; the prevention mechanisms involved use encryption algorithms to encrypt the data being transmitted, thereby preventing attackers from acquiring any useful information from the data overheard.

Whereas in active attacks the attacker tries to change or destroy the data being transmitted in the network, thereby interrupting the normal operations of the network. Active attacks can be divided into two types, external and internal attacks. External attacks can be executed by nodes from outside the network. This kind of attack can be prevented easily by using authorisation and access control mechanisms. By contrast, internal attacks are very difficult to prevent and can cause severe damage, because they come from malicious nodes who are already authorised inside the network. The security architecture proposed for VANET should therefore provide a comprehensive end-to-end security solution in order to prevent/detect data leaks. This work identifies the security requirements in VANETs, their objectives, and the methods by which they could be applied to VANETs, therefore a set of security mechanisms needs to be defined. Cryptography is one of the most powerful tools that can be used to achieve most of the security requirements, such as peer entity authentication, data origin authentication, data confidentiality, and data integrity as shown in Figure 4. The next section will show some security mechanisms that are needed to understand the work that has been done to manage and secure VANETs.

7. Security Mechanisms

These are the security mechanisms as they are defined in X.800 (Stallings USA, 2005):

- **Cryptography (Encipherment):** In this mechanism data is transformed or encrypted into a not understandable format at the sender side, by using mathematical algorithms based on one or two encryption keys, and then it is decrypted to readable format again at the receiver side.
- **Digital Signature**: In this mechanism extra data are added to the message to give the receiver a 'guarantee' that the data come from a legitimate sender, and was not altered in transmission (integrity).
- **Access Control**: A mechanism to enforce access rights to resources.
- **Authentication Exchange**: A mechanism destined to ensure the identity of an entity.
- **Traffic Padding**: A mechanism destined to frustrate traffic analysis attempts by adding extra bits into gaps in data packets.

- **Notarization**: A trusted third party (certificate authority) which is trusted by all parties to facilitate interactions to assure certain properties of data exchange.
- **Routing Control**: A mechanism used to select special securing routes for specific data and enable routing changes accordingly, particularly when a break of security is suspected.

7.1. Access Control

Protecting resources and information from unauthorised access is an important cornerstone in any information security system, this can be done by controlling how these resources and information can be accessed, otherwise unauthorized access or disclosure of confidential information especially in military systems would be an extremely damaging and fatal. So the need for access control arose because it is the first line of defence against unauthorized access to network resources and information. The purpose of using access control is to give the ability to control, monitor, restrict, and protect the confidentiality of resources and to define how users (subjects) can interact with other systems or resources and information (objects); the subject can be a user, program, or process that accesses an object, where the object can be a computer, database, or file (Harris 2007). Access control models had been divided into three models based on the mechanisms of setting the access to these objects; each model type has a different method to control accessing objects by subjects. This section explains these different models as we describe them in below:

1. **Discretionary Access Control**: Each resource (object) in Discretionary Access Control (DAC) has an owner who specifies and controls of which users (subjects) can access his resource (object), and states the permission type the subjects may have on this object. In this kind of access control model the access is restricted to the subjects based on the authorisation granted by the initial owner of this object. The initial owner of an object is the subject who created it (Sandhu & Munawer 1998). It is called Discretionary Access Control (DAC) because of the access is based on the discretion of the owner (subject); the user in this model is allowed to specify the type of access to his object.

   Access control lists (ACLs) is a form of Discretionary Access Control (DAC) which has been used in various operating systems such as Microsoft Windows, Linux, and Macintosh systems, the properties of any file in these systems have an options that allow you to control and choose which users can get an access to this resource and what the permissions may they have.

2. **Mandatory Access Control**: Subjects and data owners do not have an option to specify who can access their resources, the administrator makes that instead. Both users (subjects) in Mandatory Access Control (MAC) model have a security clearance (secret, top secret, confidential, and so on), and also data (objects) classified similarly to security clearance, these security clearances are stored in security labels, which are given to subjects and objects (Sandhu & Munawer 1998).

   Mandatory Access Control (MAC) model is arranged and stern more than in Discretionary Access Control (DAC) and found on a security label system (sensitivity). For example, a user (subject) may cleared a security level of secret, and the data (object) that been requested to access has a security label of top secret, then the user will be rejected to access this data because his security clearance (secret) is lower than the classification of the data (top secret), in order to get accessed to such this resource the subject must have a security label which is equal or higher than the security label of the object.

   This type of access control model has been used in applications where classification of information and confidentiality is essential, especially in military system where accessing the information is allowed for a specified set. Mandatory Access Control (MAC) model used in Unix systems, and

recently SE Linux which developed by the National Security Agency (NSA) (Peter Loscocco 2001).

3. **Role-Based Access Control**: In role-based access control (RBAC) model the subject will be given an access to the object based on his role or functional position (position assigned to a particular person or thing), this model is also called non-discretionary access control, because allocating a user to a role is obligatory. This means that user does not have the choice to specify what role he will be given.

   Role-based access control (RBAC) model is more complex than Discretionary Access Control (DAC), instead of specifying the access control at the object level with Access Control List (ACLs) by the subject, the administrator in (RBAC) is required to transform the policies into permission as soon as setting (ACLs). Using (RBAC) model in such these companies where the members of staff can come and leave the company in a dramatic manner is a paramount system, better than using (DAC) and (MAC) models. For example, if an x is an employee assigned to contractor role after that x left the company, then y become his replacement in this way the new replacement employee can be easily mapped to this role by the system administrator (Ferraiolo, Sandhu, Gavrila, Kuhn & Chandramouli 2001).

As we see from Figure 4 the confidentiality requirement can be solved by using encryption and routing control mechanisms, otherwise disclosing private information by a malicious node (inside the network) to unauthorised nodes will cause a fatal problem and data will be leaked. Therefore, encipherment tools (to be described in Section 8) are widely used in security systems and solve part of the problem by encrypting data exchanged between entities. Using a mechanism based on access control to ensure confidentiality, however, has still not been used, so we recommend any future research in this scope should consider using access control mechanism especially Discretionary Access Control (DAC) to ensure data confidentiality and privacy in such networks.

	Mechanism				
Requirement	Encipherment	Digital Signature	Access Control	Data Integrity	Routing Control
Authentication	Y	Y			
Access control			Y		
Confidentiality	Y				Y
Data integrity	Y	Y		Y	

(Stallings USA, 2005)

Figure 4: Relationship between security requirements and mechanisms

Most of the previous security solutions used in VANETs and MANETs focused on conventional cryptographic techniques which are the most powerful tools that can be used to achieve most of the security requirements such as authentication, data confidentiality, data integrity and non-repudiation. The next section, therefore, will give an overview of the cryptographic background to understand work already done on securing VANETs and MANETs.

8.1. Cryptographic Background

Cryptography (Stallings USA, 2005, Menezes, Van Oorschot & Vanstone 1997) is the science of encoding in cipher using specific mathematics and algorithms to encrypt and decrypt data in order to ensure secrecy and/or authenticity of messages. Using cryptography data are transformed or encrypted to

a format incomprehensible to third parties at the sender side by using mathematical algorithms based on one or two encryption keys. It is then decrypted to a readable format again at the receiver side. This enables nodes to transmit secret information through insecure networks, so that it cannot be read by any node except the intended node. The main goals of cryptography are to ensure confidentiality, integrity, authentication and non-repudiation security requirements.

In cryptography, the input to an encryption algorithm or the output of a decryption algorithm is called plaintext. Before data are sent from one node to another, the plaintext is converted into an unintelligible form which called ciphertext by the process of encryption using certain algorithms or functions. The intended receiver can then decipher/decrypt the ciphertext back into original text (plaintext) by the process of decryption. Mathematically, if M represents the plaintext message and C represents the ciphertext message as shown in Listing 1, we can say then:

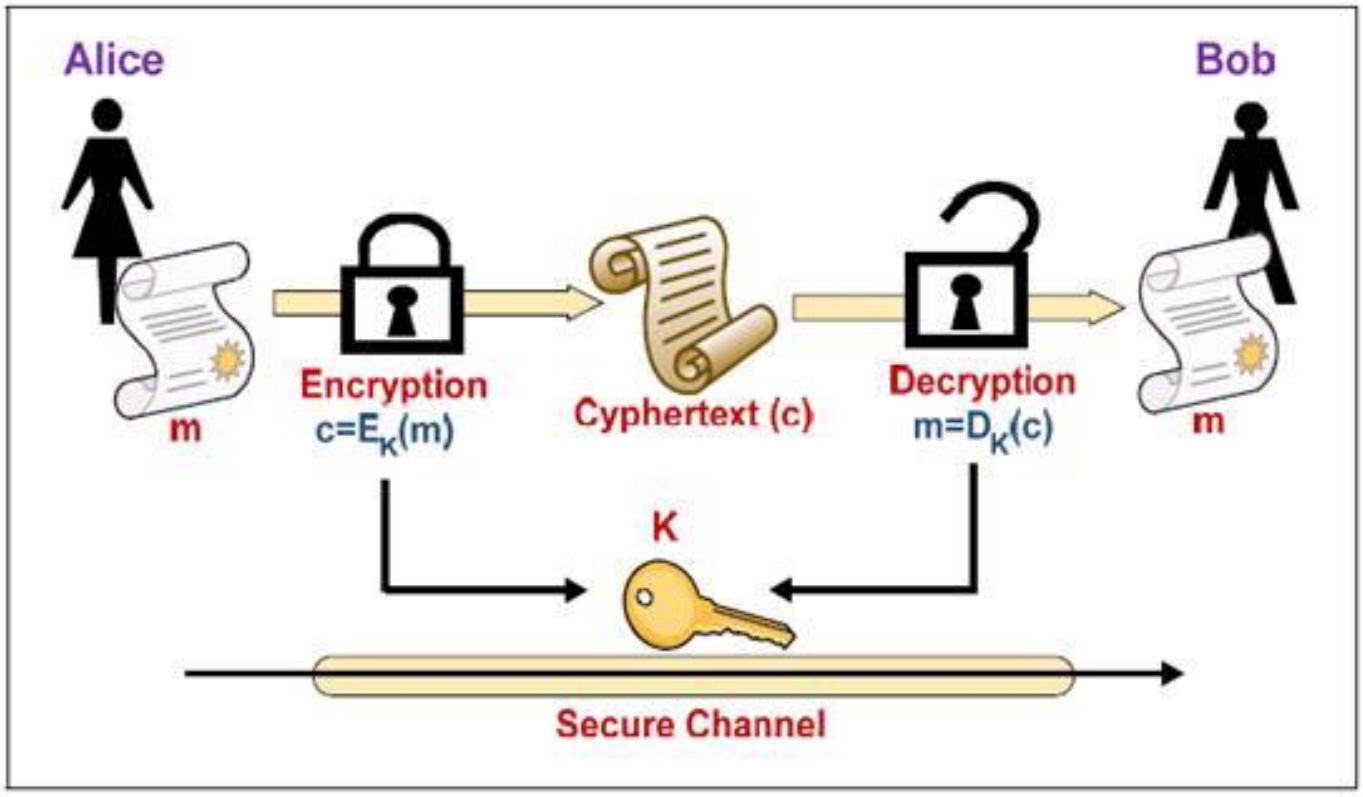
Listing 1: Encryption and decryption formulas

```
Encryption :: E(M)= C
Decryption :: D(C)= M
```

The encryption and decryption algorithms are based on keys, which are small amounts of information used by the cryptographic functions. Keys must be distributed and kept secure to ensure security of the system; this is why they are called secret keys. The security of administering the keys in cryptography science is called key management. Two main types of cryptographic algorithms are used in cryptography: symmetric key algorithms, where sender and receiver both use the same key (secret key) for encryption and decryption, whereas in asymmetric key algorithms, sender and receiver uses two different keys for encryption and decryption. These two algorithms will be discussed in the following Section 8.1 and 8.2 respectively. Digital signature, digital certificate, Public Key Infrastructure (PKI) also will be discussed in following Sections 8.2 and 8.3 respectively.

8.1. Symmetric Key Algorithms

Symmetric Key Algorithms (Stallings USA, 2005, Menezes, Van Oorschot & Vanstone 1997) are those kinds of cryptographic algorithms based on the existence of a shared key (agreed between the participants' nodes) in both the sender and receiver sides. The key used in such symmetric encryption/decryption algorithm is required to be exchanged through a secured channel. Both participants' nodes must share the same key before starting to communicate; this key can be used in both encryption and decryption processes (K) and it must be maintained secret to protect the communication afterwards. Symmetric key cryptography is the process where both sender and the receiver use the same secret key to encrypt and decrypt. An example is depicted in Figure 5 where Alice ciphers the plain text message (m) using the shared secret key (k), as a result the plaintext is changed to a ciphertext (c). Bob wants to receive the message sent from Alice in a readable format, thus he deciphers the received ciphertext (c) using the same secret key (K) which is been used in the encryption algorithm at Alice's side to change it back again to a readable format (m).



(Stallings USA, 2005)

Figure 5: Symmetric key scheme

Symmetric-key algorithms can be divided into two types: stream ciphers and block ciphers. Stream ciphers encrypt a byte of the plaintext message one at a time, whereas block ciphers encrypt a number of bytes as a single unit. Blocks of 64 bits have been previously used. Currently, however, AES (Advanced Encryption Standard) has been approved by National Institute of Standards and Technology (NIST) in 2001; it uses 128-bit blocks which replaces the commonly used Data Encryption Standard (DES) (Robles & Choi 2009, Types of Symmetric algorithms n.d.).

Generally, symmetric cryptography is much faster to execute than asymmetric cryptography. Because symmetric key algorithms require a secret key to be shared between the participants' nodes, however, any other node which 'knows' the shared secret key can decipher the messages sent in the network. The drawback of symmetric-key algorithms is thus that if the shared secret key is compromised, all messages can be deciphered which can make the whole system susceptible to attack. Therefore, the secret key in such a cryptography type needs to be altered frequently and stored securely during the key distribution process. Data integrity and non-repudiation requirements are solved by hash functions and digital signatures respectively. Key-management issues are solved by RSA (Rivest, Shamir and Adleman) encryption and by DH (Diffie-Hellman) key agreement algorithm (Types of Symmetric algorithms n.d.).

8.2. Asymmetric Key Algorithms

Asymmetric Key Algorithms (Stallings USA, 2005, Menezes, Van Oorschot & Vanstone 1997) are those kinds of cryptographic algorithms in which encryption and decryption are carried out using two different keys, one of which is referred to as the public key and the other is referred to as the private key. Asymmetric key algorithm is also termed a public key cryptography using two keys. One key is used for ciphering and the other one is used for deciphering. The decryption key is kept secret, therefore, it is

termed the "private key", whereas the encryption key is known to all participants' nodes to be able to send encrypted messages, therefore it is termed the "public key". Every node that has the public key can send encrypted messages to the node that possesses the private key, but message encrypted with the public key can be decrypted only with the corresponding private key. Both keys are related mathematically; the private key however, cannot be derived from the public key. The key management issue in symmetric key algorithm solved by public key cryptography (asymmetric key) after the idea of asymmetric algorithms was first published in 1976 by Diffie and Hellman (Diffie & Hellman 1976).

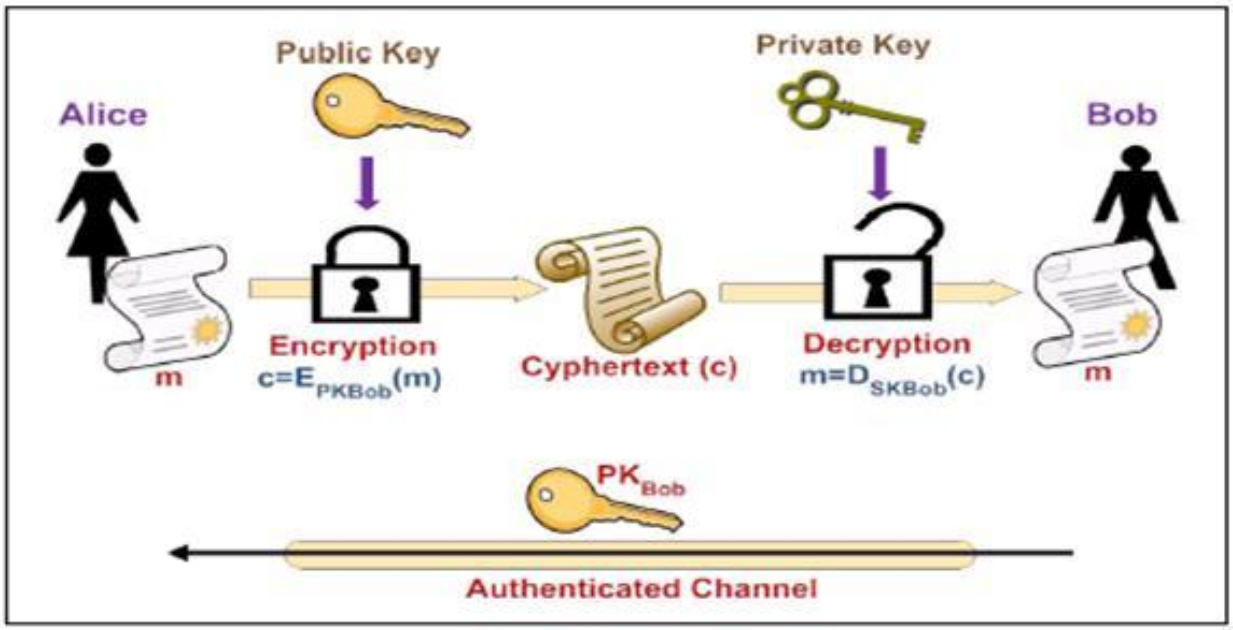


Figure 6: Asymmetric key scheme

An asymmetric key encryption scheme is depicted in Figure 6. At the start, both Alice and Bob should have an authenticated pair of public and private keys. If Alice wants to send a ciphered message m to Bob, she needs to know Bob's public key (PK[Bob]) in order to encrypt the message m and change it to a ciphertext (c). Bob is able to decrypt this ciphertext (c) using his private key (SK[Bob]) which is secret and known only to him. Public key cryptography can be divided into two subtypes which are:

- Public key encryption: a form of cryptographic system in which encryption and decryption are performed using two different keys, one to encrypt the plaintext, and another one to decrypt the ciphertext. Neither key will do both functions. When a message has been encrypted with a receiver's public key, it can be decrypted by only that receiver which has the correspondent private key. In this way the confidentiality requirement can be ensured.

- Digital signature: an approach to authenticate the identity of the sender which enables the sender of a message to attach a piece of code that functions as a signature. The signature is created by calculating the hash of the message and encrypting the message with the sender's private key. The sender's signature guarantees the source and integrity of the message sent to other nodes. Therefore, any message signed with the sender's private key can be taken to mean that the message has not been tampered with. In this way the authenticity, integrity and non-repudiation requirements can be ensured (Hunt 2001).

The main problem when using public-key cryptography is how to prove that a certain public key is genuine (belongs to the claimed node) or not, and has not been tampered with or changed by an unauthorised third party. This problem is solved using a public-key infrastructure (PKI) approach, which is an arrangement that matches public keys with respective nodes identities via a one or more group(s) of third parties, which is termed as certificate authority (CA) to authorise the ownership of key pairs (Palomar, Tapiador, Hernández-Castro & Ribagorda 2009).

Rivest, Shamir and Adleman (Rivest, Shamir & Adleman 1978) proposed a novel algorithm for obtaining digital signatures and public-key cryptosystems in 1978 which was termed afterwards as RSA. This is an example of public key cryptography based on the integer factorisation difficulty, in RSA (m) plaintext message can be encrypted or ciphertext can be decrypted using the following formula as shown in Listing 2:

Listing 2: RSA encryption and decryption formulas

```
c=m^e mod n
m=c^d mod n
```

One of the advantages of using public key cryptography (Mollin 2007, Katz & Lindell 2008) is to provide a technique for implementing digital signatures. Digital signatures give a guarantee to the receiver of a particular message that it has been sent from a node of authenticated identity, and also to ensure that the content of message is received to the intended node without it having been tampered with or changed by unauthorised modification. Digital signatures thus ensure authentication and data integrity system requirements. A digital signature also ensures non-repudiation requirement, in which the sender should not be able to deny its responsibilities of some actions. This requirement is essential especially when disputes are investigated to determine which node misbehaved. Therefore, digital signature technique is used to achieve this requirement to prove that the message was received from or sent by the alleged node.

A digital signature acts as the traditional handwritten signature. The handwritten signature however, can be imitated, whereas a digital signature is better than handwritten because it is harder to be counterfeited. It also certifies that the content of the message is received intact as well as the identity of the sender is authenticated.

As depicted in Figure 7 as a replacement of encrypting message using the receiver node's public key, digital signature encrypts the message using the sender's node's private key. Therefore, the same message can be decrypted using the sender's public key, so that tells the receiver node that the message originated from that sender. As depicted in Figure 7, if Alice wants to send an encrypted message m to Bob signed by Alice's identity, she calculates the hash digest of the message m using a specified hash function. Alice then encrypts this digest using her private key (SK[Alice]) to produce the signature and sends it with the message to Bob. When the message received at Bob's end, he recalculates the hash digest of the received message using the same hash function which was implemented at Alice's side and compares it with the hash digest generated from decrypting the signature using Alice's public key of (PK[Alice]). If both digests match that means the message m must have been created from Alice and it has not been changed or tampered with during transmission.

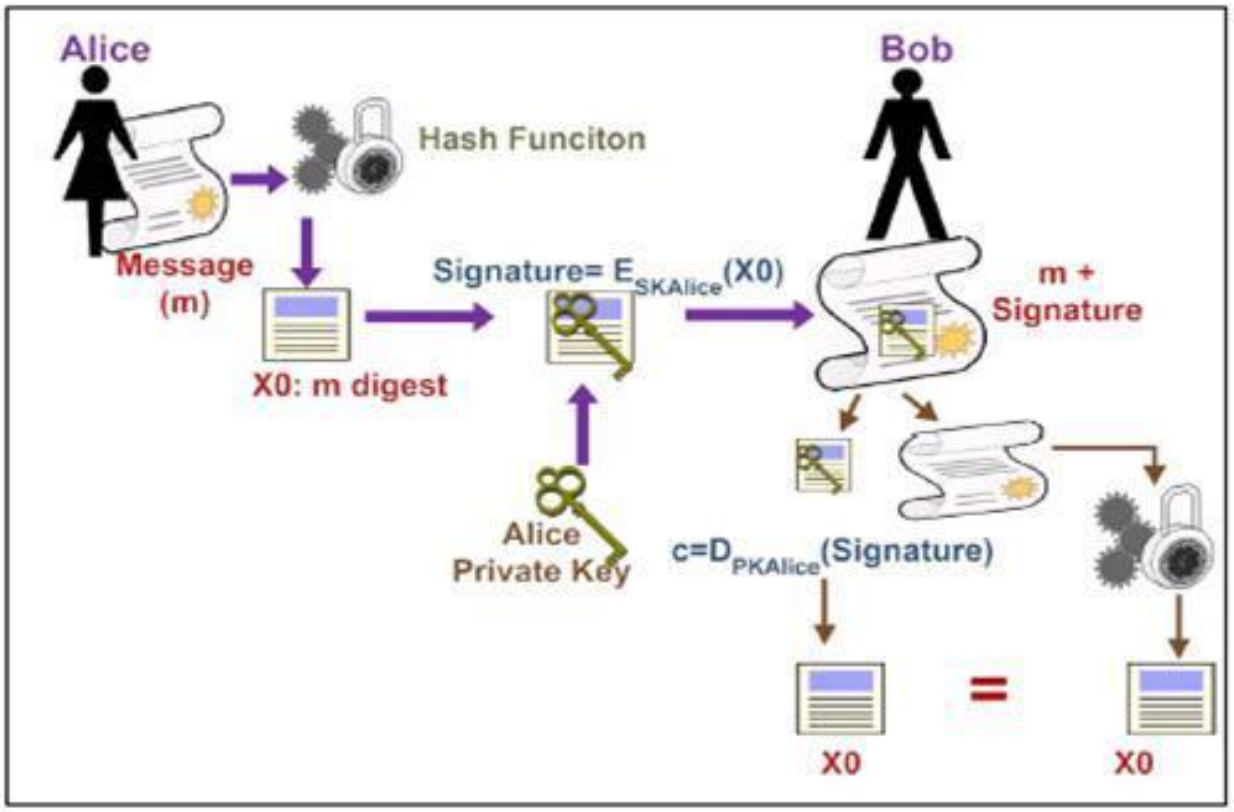


Figure 7: Digital Signature example

8.3. Digital Certificate

The Digital Certificate is an electronic document used for establishing the credentials of a node (i.e. certify the identities of nodes) which combines a digital signature to match between the public key and the nodes' identification to verify the nodes' identities. It is issued and certified by one or more certification authorities (CAs) (Digital Certificates n.d.a, Digital Certificates n.d.b). In public cryptographic system nodes need to make sure that they are ciphering to legitimate identities of nodes. The important of digital certificates comes from protecting the network from the man-in-the-middle attack scenario. The man-in-the-middle attack is a potential threat in such environments where keys exchanged between nodes and servers can enable the attacker to insert, read, and modify messages sent among two victim nodes without either node being aware of the connection they have used has been compromised. In this type of attack the attacker makes autonomous links with the victims to play with messages sent between them. Victim nodes believe that they are communicating directly and securely between each other, when in fact the entire connection is managed by the attacker (Stallings USA, 2005).

For instance, if Alice wants to send a message to Bob securely, she will ask for Bob's public key. If Emma (the attacker) can find the public key of Bob and be able to intercept the messages sent between Alice and Bob, the man-in-the-middle attack can be mounted. First, Emma will impersonate the identity of Bob and send her public key to Alice as if it were Bob's public key. This will make Alice believe that it belongs to Bob and she will use it to encrypt the message and then send it back to Bob. This encrypted message will be intercepted by Emma (Almomani August 2007).

This time Emma ciphers the message using her private key, keeps a copy of it and re-ciphers it using the correct public key of Bob. Once the message is received by Bob, he will believe that it was sent by Alice.

This scenario shows simply the need for some method of ensuring that Alice and Bob have genuinely used each other's public keys and not the attacker's public key. If not, they will remain vulnerable to such an attack. Digital certificates therefore are used to prevent this kind of attack happening. They are like the traditional identification cards such as passports and drivers' licenses which can verify the identities of their owners'. Similar to traditional identification cards which are issued by identified government authorities, digital Certificates in MANETs and VANETs are also issued by trusted third parties. A digital Certificate verifies the identity of the node but instead of including a photo and a signature of the certificate's owner, digital certificates bind the owner's public key to the owner's private key. Therefore, digital certificates contain node identification, serial number, expiry date, public key, and digital signature of the certification authority (CA) which issued the certificate. This signature in the certificate act as attestation by the certificate's signer that the information of node and the public key belong together (Al-Bayatti February 2009).

In order to make a digital signature, a certification authority (CA) employs its private key to digitally sign each certificate it issues. The CA creates a message digest from the certificate using a specified hash function, and then encrypts this digest with its private key, and inserts the digital signature inside the certificate. When the certificate is received at the node, the node recalculates the hash digest of the received certificate using the same hash function which was implemented by the CA, and then compares it with the hash digest generated from decrypting the certificate using the CA's public key to verify the certificate's integrity. If both digests match, that means the certificate must have been created from the CA and has not been changed or tampered with during transmission. If they do not match then the certificate is not original or has been issued from a non certified authority (Digital Certificates n.d.a).

9. State of the Art

In comparison with wired networks where the devices must have a physical access to the network medium, mobile ad hoc networks have no apparent secure boundary. There is no need for the attackers to have a physical access to the network; once the attackers are in the transmission range of any other devices, then they can join and communicate with other devices. According to the nature of mobility in ad hoc networks, liberty to join, moving outside and inside the networks makes MANETs vulnerable to attacks, which can result from any device in the same transmission range (Carvalho 2008). In comparison with wired networks where the nodes can get electrical supply directly from the power points, in MANETs nodes are generally operated by small batteries with limited lifetime. This makes nodes unable to perform intensive computations over prolonged periods of time. An attacker on the other hand is typically able to provide sufficient power-supply and thus must be assumed to be able to perform intensive computations (Mehul & Limaye 2009), meaning that attack and defence in these networks is not equally matched. The lack of centralized management in MANETs makes detection of attacks difficult, since they are highly dynamic and large scale therefore they cannot be easily monitored; benign (non-malignant) failures in the MANETs are also fairly common, for example transmission destructions and packet dropping. As a result, malicious failures will be more difficult to discover. Since security is an essential component in a hostile environment, these unique characteristics of MANETs raise challenges that security requirements must address (Yang, Luo, Ye, Lu & Zhang 2004, Djenouri, Khelladi & Badache 2005).

There has been appreciable work by the research community (Yang, Luo, Ye, Lu & Zhang 2004, Burbank, Chimento, Haberman & Kasch 2006, Zhou & Haas 1999, Hubaux, Buttyán & Capkun 2001, Capkun, Buttyán & Hubaux 2003) in message encryption, digital signature, and key management. Many challenges particularly related to the privacy and data confidentiality of originator, however, remain to be solved. These available approaches which have been used in MANETs such as access control, digital signature, and encryption focused only in securing the channel during the transmission, however how these nodes act after and use this information has been mostly neglected.

Most research on security in VANETs addressed location privacy (Sampigethaya, Li, Huang & Poovendran 2007, Yan & Chen 2010) and 'big brother' scenarios (Raya & Hubaux 2005) where location of nodes can be tracked by an untrusted third party. The CARAVAN scheme (Sampigethaya, Huang, Li, Poovendran, Matsuura & Sezaki 2005) allows mobile nodes to maintain privacy by forming groups in which the group leader acts as a proxy on behalf of all members of the group with a random silent period to mitigate tracking of nodes. Others (Dotzer 2006, Gerlach & Guttler Dublin, 2007, Tang & Hong n.d.) addressed the same problem by using pseudonyms to hide the relationship between the identity and the location. Although pseudonyms are significant in overall security of VANETs are advantageous for protecting the identity, these solutions do not provide full security for VANETs in term of data confidentiality, as they cannot control the dissemination of information. Indeed for many application-level services the knowledge of the senders' identity is paramount to their function. Hence, pseudonyms could only be one part of a privacy solution, but the need for more comprehensive solution(s) allowing originators of information control over its dissemination, remains to be solved.

In addition, a few academic papers have been published by Raya's group et al to provide a general survey of crucial security issues, giving an overview of challenges, adversaries, attacks, properties of VANET, and useful security mechanisms to design robust solutions (Raya & Hubaux 2005, Raya & Hubaux 2007). In later research (Raya, Papadimitratos & Hubaux 2006) they proposed a secure architecture in VANET to adress these issues.

Existing approaches to security of MANETs include traditional cryptographic solutions using public key certificates (Li & Wang n.d., Wu, Chen, Wu & Cardei 2007) to maintain trust, in which a Trusted Third Party (TTP) or Certificate Authority (CA) certifies the identity associated with a public key of each communicated entity, Almomani and Zedan (Almomani & Zedan 2007) proposed a comprehensive, top-down, end-to-end security solution for MANET based upon a well defined architecture and exploiting two of the ITU-T recommendations: X.800, and X.805. Such approaches can therefore, provide end-to-end secure communication channels. These approaches mainly focused on message confidentiality, integrity and non-repudiation, they do not consider however the trust management of the communicated entities, and how these certified entities act is left to the application layer (Blaze, Feigenbaum & Lacy 1996). Therefore, Al-Bayatti et al (Al-Bayatti, Zedan & Cau 2009) proposed behaviour detection algorithm combined with threshold cryptography digital certificates to satisfy prevention and detection to securely manage Mobile Ad hoc Network of Networks (MANoNs), whereas Zhou and Haas (Zhou & Haas 1999) studied the security threats, vulnerabilities and challenges which faces the ad hoc network. In their work (Zhou & Haas 1999) they protected the packets sent between nodes by choosing the secure routing path to the destination node based on the redundancies routes between nodes to maintain the availability requirement. This is because all key-based cryptographic approaches such as digital signature need a proper and secure key management scheme to bind between the public and private keys to the nodes in the network; Zhou and Haas subsequently used replication and new cryptographic technique (threshold cryptography) (Desmedt 1994, Desmedt & Frankel 1990) to build a secure key management process to achieve the trust between a set of servers in ad hoc networks by distributing trust among aggregation of nodes to certify nodes are trustworthy.

Securing the routing in MANETs has also been given much attention by the researchers; many approaches, therefore, have been proposed to deal with external attack. Sirios and Kent (Sirois & Kent 1997) proposed an approach to protect the packet sent to multi receivers by using keyed one-way hash function supported by windowed sequence number to ensure data integrity.

In an analogous context of commercial and medical environments, individuals also demand that their personal information such as their names, addresses, phone numbers, national insurance numbers, credit card details, passwords, or date of birth (DOB) are transmitted confidentially. In particular they need

assurance that these sensitive data have been securely communicated to the appropriate persons or organisations and to no others. Therefore, Pearson and Mont (Pearson & Casassa-Mont 2011) employed a clever idea of sticking policies with data to control how the personal information should be processed, handled, shared with other specified parties.

10. Summary

This chapter presented a review of wireless ad hoc networks and mobile ad hoc networks (MANETs); it also described the characteristics, challenges, vulnerabilities of mobile ad hoc network, and then numerated the applications of MANET. This chapter also presented an introduction of the vehicle ad hoc networks (VANETs), history and background, also it described the characteristics and challenges of vehicle ad hoc network, this chapter also provided a comparison between characteristics of MANETs and VANETs as described in the Table 1.

Although VANETs and MANETs are interesting for many applications, they nevertheless have several challenges. Each of these challenges can be considered as a separate research area needing intensive investigation. Researchers investigated the security issues in both MANETs and VANETs and they proposed many solutions; this chapter therefore this chapter highlighted the network security concepts: security requirements, security attacks and security mechanisms, it also presented an overview of the cryptography background, and presented the related work in privacy and confidentiality issues in both VANETs and MANETs. Finally, this chapter presented some of the previous work (State of the Art) on securing VANETs and MANETs.

References

Al-Bayatti, A. H. (February 2009), Security management for mobile ad hoc network of networks (MANoN), PhD thesis, De Montfort University.

Al-Bayatti, A., Zedan, H. & Cau, A. (2009), Security solution for mobile ad hoc network of networks (manon), *in* 'Networking and Services, 2009. ICNS '09. Fifth International Conference on', pp. 255 –262.

Al-Jaroodi, J. (2002), Security issues at the network layer in wireless mobile ad hoc networks at the network layer, Technical report, Faculty of Computer Science and Engineering, University of Nebraska-Lincoln, Nebraska, USA.

Aldabbas, H., Alwada'n, T., Janicke, H. & Al-Bayatti, A. (2012), 'Data confidentiality in mobile ad hoc networks', *International Journal of Wireless and Mobile Networks (IJWMN), 4, (1), pp. 225-236* .

Aldabbas, H., Janicke, H., AbuJassar, R. & Alwada'n, T. (2012), Ensuring data confidentiality and privacy in mobile ad hoc networks, *in* 'Advances in Computer Science and Information Technology. Networks and Communications', Springer, pp. 490–499.

Almomani, I. M. (August 2007), Security Solutions for Wireless Mobile Ad hoc Networks(WMANET), PhD thesis, De Montfort University.

Almomani, I. & Zedan, H. (2007), 'End-to-end security solution for wireless mobile ad hoc network (wmanet)'.

Andrews, J. G., Ghosh, A. & Muhamed, R. (2007), *Fundamentals of WiMAX: Understanding Broadband Wireless Networking (Prentice Hall Communications Engineering and Emerging Technologies Series)*, Prentice Hall PTR, Upper Saddle River, NJ, USA.

Bai, F. & Krishnan, H. (2006), Reliability analysis of DSRC wireless communication for vehicle safety applications, *in* 'Intelligent Transportation Systems Conference, 2006. ITSC'06. IEEE', IEEE, pp. 355–362.

Bharathidasan, A. & Ponduru, V. (2002), Sensor networks: An overview, Technical report, Department of Computer Science, University of California, Davis, USA. wwwcsif.cs.ucdavis.edu/~bharathi/sensor/survey.pdf

Biswas, S., Tatchikou, R. & Dion, F. (2006), 'Vehicle-to-vehicle wireless communication protocols for enhancing highway traffic safety', *Communications Magazine, IEEE* **44**(1), 74–82.

Blaze, M., Feigenbaum, J. & Lacy, J. (1996), Decentralized trust management, *in* 'Proceedings of the 1996 IEEE Symposium on Security and Privacy', IEEE Computer Society Press, pp. 164–173.

Burbank, J., Chimento, P., Haberman, B. & Kasch, W. (2006), 'Key challenges of military tactical networking and the elusive promise of manet technology', *Communications Magazine, IEEE* **44**(11), 39–45.

Capkun, S., Buttyán, L. & Hubaux, J. (2003), 'Self-organized public-key management for mobile ad hoc networks', *Mobile Computing, IEEE Transactions on* **2**(1), 52–64.

Carcelle, X., Dangand, T. & Devic, C. (2006), *Ad-Hoc Networking*, Vol. 212/2006 of *IFIP International Federation for Information Processing*, Springer, Santiago, Chile, chapter Wireless Networks in industrial environments: State of the art and Issues, pp. 141–156.

Carvalho, M. (2008), 'Security in mobile ad hoc networks', *Security Privacy, IEEE* **6**(2), 72 –75.

Chadha, R. & Kant, L. (2007), *Policy-Driven Mobile Ad hoc Network Management*, Wiley-IEEE Press.

Desmedt, Y. (1994), 'Threshold cryptography', *European Transactions on Telecommunications* **5**(4), 449–458.

Desmedt, Y. & Frankel, Y. (1990), Threshold cryptosystems, *in* 'Advances in Cryptology—CRYPTO'89 Proceedings', Springer, pp. 307–315.

Diffie, W. & Hellman, M. (1976), 'New directions in cryptography', *Information Theory, IEEE Transactions on* **22**(6), 644–654.

Digital Certificates (n.d.*a*), http://technet.microsoft.com/en-us/library/cc962029.aspx. Accessed June 15, 2012.

Digital Certificates (n.d.*b*), http://www.webopedia.com/TERM/D/digital_certificate.html. Accessed June 15, 2012.

Djenouri, D., Khelladi, L. & Badache, N. (2005), 'A survey of security issues in mobile ad hoc networks', *IEEE communications surveys* **7**(4).

Dotzer, F. (2006), Privacy issues in vehicular ad hoc networks, *in* 'Privacy Enhancing Technologies', Springer, pp. 197–209.

Ferraiolo, D., Sandhu, R., Gavrila, S., Kuhn, D. & Chandramouli, R. (2001), 'Proposed NIST standard for role-based access control', *ACM Transactions on Information and System Security (TISSEC)* **4**(3), 224–274.

Fiore, M., Harri, J., Filali, F. & Bonnet, C. (2007), Vehicular mobility simulation for VANETs, *in* 'Simulation Symposium, 2007. ANSS'07. 40th Annual', IEEE, pp. 301–309.

Gast, M. (2005), *802.11 wireless networks: the definitive guide*, O'Reilly Media, USA.

Gerlach, M. & Guttler, F. (Dublin, 2007), Privacy in VANETs using changing pseudonyms-ideal and real, *in* 'Vehicular Technology Conference, 2007. VTC2007-Spring. IEEE 65th', IEEE, pp. 2521–2525.

Ghosh, A., Wolter, D., Andrews, J. & Chen, R. (2005), 'Broadband wireless access with wimax/802.16: current performance benchmarks and future potential', *Communications Magazine, IEEE* **43**(2), 129–136.

Harris, S. (2007), *CISSP all-in-one exam guide*, McGraw-Hill Osborne Media.

Hubaux, J., Buttyán, L. & Capkun, S. (2001), The quest for security in mobile ad hoc networks, *in* 'Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing', ACM, pp. 146–155.

Hunt, R. (2001), Pki and digital certification infrastructure, *in* 'Networks, 2001. Proceedings. Ninth IEEE International Conference on', pp. 234 – 239.

Janicke, H., Sarrab, M. & Aldabbas, H. (2012), Controlling data dissemination, *in* 'Data Privacy Management and Autonomous Spontaneus Security', Springer, pp. 303–309.

Jiang, D., Taliwal, V., Meier, A., Holfelder, W. & Herrtwich, R. (2006), 'Design of 5.9 GHz DSRC-based vehicular safety communication', *Wireless Communications, IEEE* **13**(5), 36–43.

Katz, J. & Lindell, Y. (2008), *Introduction to modern cryptography*, Chapman & Hall.

Killat, M., Schmidt-Eisenlohr, F., Hartenstein, H., Rossel, C., Vortisch, P., Assenmacher, S. & Busch, F. (2007), Enabling efficient and accurate large-scale simulations of vanets for vehicular traffic management, *in* 'Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks', VANET '07, ACM, New York, NY, USA, pp. 29–38.
http://doi.acm.org/10.1145/1287748.1287754

Lehr, W. & McKnight, L. (2003), 'Wireless Internet access: 3G vs. WiFi', *Telecommunications Policy, Research Program on Internet and Telecoms Convergence, Massachusetts Institute of Technology (MIT)* **27**(5-6), 351–370.

Li, F. & Wang, Y. (2008), 'Routing in vehicular ad hoc networks: A survey', *Vehicular Technology Magazine, IEEE* **2**(2), 12–22.

Li, S. & Wang, X. (n.d.), 'Enhanced security design for threshold cryptography in ad hoc network'.

Li, W. & Joshi, A. (2004), 'Security issues in mobile ad hoc networks-a survey', *White House Papers Graduate Research In Informatics at Sussex* **17**, 1–23.

Manui, S. & Kakkasageri, M. (2008), 'Issues in mobile ad hoc networks for vehicular communication', *IETE (INSTITUTE OF ELECTRONICS & TELECOMMUNICATION) Technical Review* **25**(2), 59.

Mehul, E. & Limaye, V. (2009), Security in mobile ad hoc networks, *in* 'Handbook of Research in Mobile Business Second edition: Technical, Methodological and Social Perspectives Ed. Bhuvan Unhelkar', Hershey: IGI Global, pp. 541–558.

Menezes, A., Van Oorschot, P. & Vanstone, S. (1997), *Handbook of applied cryptography*, CRC.

Mishra, A. & Nadkarni, K. (2003), Security in wireless ad hoc networks, *in* 'The handbook of ad hoc wireless networks', CRC Press, Inc., pp. 499–549.

Misra, S., Woungang, I. & Misra, S. C. (2009), *Guide to Wireless Ad Hoc Networks*, Springer-Verlag New York Inc.

Mollin, R. (2007), *An introduction to cryptography*, CRC Press.

Murthy, C. S. R. & Manoj, B. (2004), *Ad Hoc Wireless Networks: Architectures and Protocols*, Prentice Hall PTR, Upper Saddle River, NJ, USA.

Oates, J. (2011), 'Toyota and microsoft ink e-car deal in a cloud of telematics', http://www.theregister.co.uk/2011/04/07/microsoft_toyota/. Accessed July 8, 2011.

Olariu, S. & Weigle, M. (2009), *Vehicular Networks from Theory to Practice*, Chapman & Hall, USA.

Palomar, E., Tapiador, J., Hernández-Castro, J. & Ribagorda, A. (2009), '17 cooperative security in peer-to-peer and mobile ad hoc networks', *Cooperative Wireless Communications ed by Yan Zhang, Hsiao-Hwa Chen, Mohsen Guizani* p. 391.

Papadimitratos, P. & Haas, Z. J. (2003), *Securing mobile ad hoc networks*, CRC Press, Inc., Boca Raton, FL, USA, pp. 551–567. http://dl.acm.org/citation.cfm?id=989711.989743

Pearson, S. & Casassa-Mont, M. (2011), 'Sticky policies: An approach for privacy management across multiple parties', *Computer Society* **1**(99), 60–68.

Peter Loscocco, N. (2001), Integrating Flexible Support for Security Policies into the Linux Operating System, *in* 'Proceedings of the FREENIX Track: 2001 USENIX Annual Technical Conference, June 25-30, 2001, Boston, Massachusetts, USA', USENIX Association, p. 29.

Raya, M. & Hubaux, J.-P. (2005), The security of vehicular ad hoc networks, *in* K. P. Laberteaux, H. Hartenstein, D. B. Johnson & R. Sengupta, eds, 'Vehicular Ad Hoc Networks', ACM, pp. 93–94. http://dblp.uni-trier.de/db/conf/mobicom/vanet2005.html#RayaH05

Raya, M. & Hubaux, J.-P. (2007), 'Securing vehicular ad hoc networks.', *Journal of Computer Security* **15**(1), 39–68.
http://dblp.uni-trier.de/db/journals/jcs/jcs15.html#RayaH07

Raya, M., Papadimitratos, P. & Hubaux, J.-P. (2006), 'Securing vehicular communications', *Wireless Communications, IEEE* **13**(5), 8 –15.

Rivest, R. L., Shamir, A. & Adleman, L. (1978), 'A method for obtaining digital signatures and public-key cryptosystems', *Commun. ACM* **21**, 120–126.
http://doi.acm.org/10.1145/359340.359342

Robles, R. & Choi, M. (2009), 'Symmetric-key encryption for wireless internet scada', *Security Technology* pp. 289–297.

Sampigethaya, K., Huang, L., Li, M., Poovendran, R., Matsuura, K. & Sezaki, K. (2005), Caravan: Providing location privacy for vanet, *in* 'in Embedded Security in Cars (ESCAR)', Citeseer.

Sampigethaya, K., Li, M., Huang, L. & Poovendran, R. (2007), 'Amoeba: Robust location privacy scheme for vanet.', *IEEE Journal on Selected Areas in Communications* **25**(8), 1569–1589.

Sandhu, R. & Munawer, Q. (1998), How to do discretionary access control using roles, *in* 'Proceedings of the third ACM workshop on Role-based access control', RBAC '98, ACM, New York, NY, USA, pp. 47–54. http://doi.acm.org/10.1145/286884.286893

Sarkar, S. K., Basavaraju, T. G. & Puttamadappa, C. (2007), *Ad Hoc Mobile Wireless Networks: Principles, Protocols and Applications*, Auerbach Publications, Boston, MA, USA.

Sirois, K. & Kent, S. (1997), Securing the nimrod routing architecture, *in* 'sndss', Published by the IEEE Computer Society, p. 74.

Stallings, W. (USA, 2005), *Cryptography and Network Security: Principles and Practice*, 4rd edn, Pearson Education.

Tang, L. & Hong, X. (n.d.), 'Protecting location privacy by camouflaging movements'.

Toh, C. (2001), 'Maximum battery life routing to support ubiquitous mobile computing in wireless ad hoc networks', *IEEE communications Magazine* **39**(6), 138–147.

Wisitpongphan, N., Bai, F., Mudalige, P. & Tonguz, O. (2007), On the routing problem in disconnected vehicular ad-hoc networks, *in* 'INFOCOM 2007. 26th IEEE International Conference on Computer Communications', IEEE, pp. 2291–2295.

Wu, B., Chen, J., Wu, J. & Cardei, M. (2007), 'A survey of attacks and countermeasures in mobile ad hoc networks', *Wireless Network Security* pp. 103–135.

Xing, F. & Wang, W. (2007), Understanding Dynamic Denial of Service Attacks in Mobile Ad Hoc Networks, *in* 'Military Communications Conference, 2006. MILCOM 2006. IEEE', IEEE, pp. 1–7.

Yan, Z. & Chen, Y. (2010), 'Adcontrep: a privacy enhanced reputation system for manet content services', *Ubiquitous Intelligence and Computing* pp. 414–429.

Yang, H., Luo, H., Ye, F., Lu, S. & Zhang, L. (2004), 'Security in mobile ad hoc networks: challenges and solutions', *Wireless Communications, IEEE* **11**(1), 38–47.

Yick, J., Mukherjee, B. & Ghosal, D. (2008), 'Wireless sensor network survey', *Computer Networks* **52**(12), 2292–2330.

Yousefi, S., Bastani, S. & Fathy, M. (2007), On the performance of safety message dissemination in vehicular ad hoc networks, *in* 'IEEE: Proceedings of 4th European Conference on Universal Multiservice Networks ECUMN'2007', pp. 377–390.

Zhang, Y. & Lee, W. (2005), 'Security in mobile ad-hoc networks', *Ad Hoc Networks* pp. 249–268.

Zhou, L. & Haas, Z. (1999), 'Securing ad hoc networks', *Network, IEEE* **13**(6), 24–30.

ADDITIONAL READING

C. Siva Ram Murthy and B.S. Manoj. Ad Hoc Wireless Networks: Architectures and Protocols. Prentice Hall PTR, Upper Saddle River, NJ, USA, 2004.

Subir Kumar Sarkar, T. G. Basavaraju, and C. Puttamadappa. Ad Hoc Mobile Wireless Networks: Principles, Protocols and Applications. Auerbach Publications, Boston, MA, USA, 2007.

Saleh Yousefi, Mahmoud Siadat Mousavi, and Mahmood Fathy. Vehicular ad hoc networks (vanets): Challenges and perspectives. In ITS Telecommunications Proceedings, 2006 6th International Conference on, pages 761 –766, june 2006.

KEY TERMS AND DEFINITIONS

MANET: Mobile ad hoc network (MANET).

VANET: Vehicular ad hoc network (VANET).