Noname manuscript No.
(will be inserted by the editor)

Security issues in self-organized ad-hoc networks (MANET, VANET, and FANET): A survey

Sihem GOUMIRI · Mohamed amine RIAHLA · M'hamed HAMADOUCHE

Received: date / Accepted: date

Abstract Self-organized AdHoc networks have become one of the most interested and studied domains, especially with the rapid development of communication technologies and electronic devices. These networks regroup wireless and self-configuring nodes that communicate independently without a fixed infrastructure. Many applications operate with the AdHoc network due to its rapid deployment and low costs. Security in AdHoc networks is a crucial aspect that protects the exchanges between users and improves network performances. In this paper, a presentation of three AdHoc networks: MANET (Mobile AdHoc Network), VANET (Vehicle AdHoc Network), and FANET (Flaying AdHoc Network) is performed with the focus on their security issues. The paper blends the security requirements and the different attacks faced to the three reviewed networks.

Keywords Security · Self-organized networks · AdHoc networks · MANET · VANET · FANET

1 Introduction

A self-organized AdHoc network is a dynamic, autonomous, and wireless system com-posed of a group of mobile devices able to communicate independently in the network area [1]. Each mobile device is an autonomous and self-configuring node that acts in the network without needing any central administration [1][2]. The number of nodes and links is varied over time, which

Sihem GOUMIRI
University of Boumerdes, Ingénierie des Systèmes et Télécommunications Laboratory, 35000 Boumerdes, ALGERIA
E-mail: s.goumiri@univ-boumerdes.dz

Mohamed amine RIAHLA · M'hamed HAMADOUCHE
University of Boumerdes, LIMOSE Laboratory, South Campus, 35000 Boumerdes, ALGERIA

frequently changes the network topology. Recently, these networks are present in many fields and applications because they offer great benefits like rapid deployment and low costs. A self-organized AdHoc network is a large definition that gathers very diverse network technologies like those introduced in this survey: MANET (Mobile Ad hoc network), VANET (Vehicular Ad hoc Network), and FANET (Flaying AdHoc network). These networks encountered many serious problems and challenges about maintaining the normal function of the network or improving its performances. Indeed, ensuring security in such an environment is the greatest challenge for searchers. The network must be resilient to different risks and provide many alternative solutions faced with attacks. In addition, nodes and data must be present in a safe environment to accomplish a predefined mission or ensure the purpose of the network deployment. This paper reviews the security issues and requirements in the self-organized AdHoc networks (MANETs, VANETs, and FANETs). The remaining parts of this survey are planned as follows: The first section presents background about three existing and popular AdHoc networks (MANETs, VANETs, and FANETs). The second section describes the security issues and services in AdHoc networks. The third section lists the potential attacks and threats on MANET, VANET, and FANET. The last section concludes the paper and designates our future direction of searches.

2 Self-organized AdHoc networks

2.1 Background

In the last years, the AdHoc network interested industry and academia due to its intended fields of application. By adjusting dimensional parameters and using new technologies of devices, new AdHoc network subcategories emerged like MANET (Mobile Ad hoc network), VANET (Vehicles Ad hoc network), and FANET (Flying Ad hoc network).

MANET (Mobile Ad hoc network) [3] is a wireless mobile system composed of nodes that communicate with wireless links fig.1. Its main characteristics are the absence of any fixed infrastructure and the self-configuring nodes, which makes them able to establish communications, exchange information, and ensure network functionalities. The network size of MANET is frequently changed over time due to nodes newly joined the networks and those dynamically leaved (roaming). Today with the popularity of mobile devices (smartphones, sensors, pc, etc.) MANET is present in many military and civil fields like room class conferences, emergency rescue operations, and military control.

VANET (Vehicular AdHoc Network) is a technology for managing road traffic and providing a safe driving environment [4]. The network is composed of a set of vehicles present in the road fig.2. Vehicles communicate and exchange information with each other by using two communication modes. The first one is direct Vehicle-to-Vehicle communication (V2V) that allows estab-

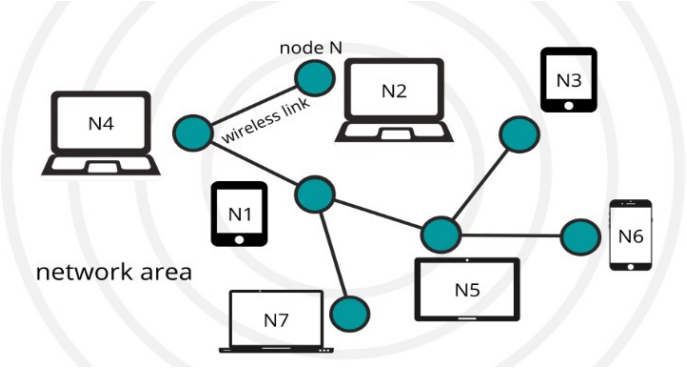

Fig. 1 Mobile AdHoc network (MANET

lishing immediate communication between vehicles in the same network. The second mode is a vehicle to interface (V2I) that requires the connection to a fixed infrastructure unit called RSU (roadside unit). This interface allows communication between vehicles, monitors them, and provides them access to the Internet cloud.

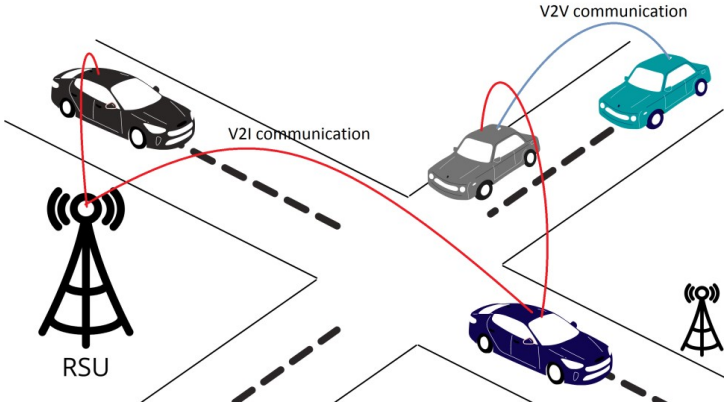

Fig. 2 Vehicles AdHoc network (MANET

FANET (Flying AdHoc Networks) is a subset of MANETs that uses Ad-Hoc communication in a three dimensional plane. The network is composed of a collection of UAVs (Unmanned Aerial Vehicles) [5] able to execute a predefined mission fig.3. UAVs are small aerial vehicles equipped with sensors and advanced computing devices. FANET inherits the same features of MANET except that nodes can fly autonomously in the network producing higher mobility degrees. Two communication modes are distinguished: Air-to-air wireless communications (A2A) using the AdHoc mode and air-to-ground wireless communications (A2I) using infrastructures like ground stations or satellites.

Overall, this portion of networks is called to en-sure dangerous tasks related to disasters, target detection for security services or rescue operations, monitoring, etc.

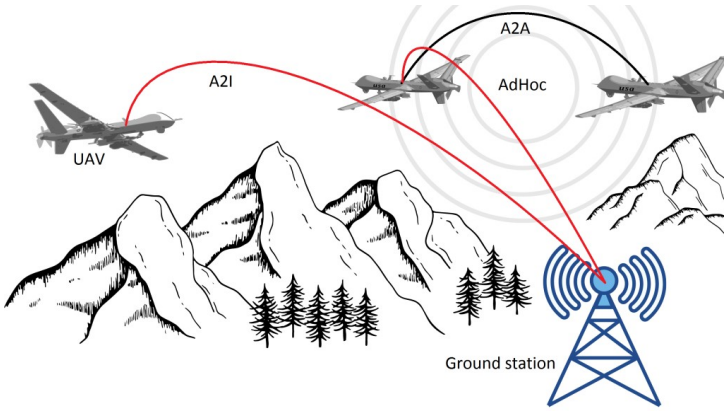

Fig. 3 Flaying AdHoc network (MANET

2.2 Main features

Self-organized AdHoc networks introduced in this paper have some features in common. The main ones are:

- The self-organized nodes ;
- The use of existing nodes for managing the network traffic (i.e. node acts as hosts and routers at the same time) ;
- The multi-hop rooting to transfer information;
- The limited physical security due to the movement of nodes.

Other specific characteristics that make the difference between MANETs, VANETs, and FANETs are listed in table 1 as follow:

- The nodes used in the network: heterogeneous or homogeneous in type, nodes interacted in dynamic networks are numerous and depend on the purpose of designing the network. Vehicles, sensor devices, or UAVs are the famous types of equipment that could be present with the existing networks;
- The environment dimension: this indicates the movements of nodes in the coverage area of the network. In some technologies, nodes move close to the ground, and in others, nodes can fly in free space;
- The speed of nodes: random, height, or slow movements of nodes characterize networks. This metric identifies the mobility level that changes the network topology;

Table 1 Differences between the network features

Networks	Nodes	environment	node speed	Node energy	Node density
Manet	PC, sensor, smart phone	Random 2-D	Lower	Low	Low
Vanet	Vehicles	linear trajectory 2-D	Higher	High	High
Fanet	UAVs sys-tems	Random 3-D	Most higher	High	Low

– The energy of nodes: This feature differs for each dynamic network. Depending on the mission of nodes, some technologies require devices with a High capacity of energy, but others tolerate equipment with a low capacity of energy.

3 Security issues and services

Security is an important factor and a veritable challenge in dynamic networks [6]. The main objective here is to preserve the security of nodes, data, and services. Indeed, the network must protect core services [7] that ensure some policies and requirements. It includes authentication, privacy, and non-repudiation of nodes on the one hand and integrity and confidentiality of the exchanged data on the other hand. Moreover, the network must be resilient faced with different attacks. These objectives are challenged in the AdHoc mode due to its specific feature previously detailed. The services of self-organized AdHoc networks (MANET- VANET- FANET) to be protected are highlighted and defined bellows:

– Availability refers to ensure the operation of the service provided by the network [6]. The network must ensure the role of all nodes during their life cycle (even those attacked). Before deploying any dynamic networks, it is essential to implement alternate solutions that always ensure communications between nodes in case of attacks.
– Authentication provides trustable communications between the network nodes. This service ensures the real identity of nodes by using methods like certification [8]. Researches in this area are numerous and handled many challenges because of the limited features of dynamic networks.
– Confidentially is the way to define permissions that allow nodes accessing to a specified data and services. This service ensures transiting information securely between nodes [8]. The main application to ensure confidentiality employs encryption methods. However, improving this service in dynamic networks is challengeable, making researches always opened.

– Integrity means not manipulate the message circulated in the network. Therefore, attacks against integrity attempt to modify or delete the content of packets transiting between nodes [[6].
– Non-repudiation service associates delivered data and behavior to the correct node that sent any packet in the network [8]. Such a service is essential to have traceability and prevent erasing information related to an attack.

4 Attacks on AdHoc networks

Various attacks against AdHoc networks were examined [9][10][11] in this paper. All these attacks share similar effects that paralyze the network services and degrade performances. Depending on the status, the behavior, or the purpose of the attacker, authors in [12] define three attacks classifications. In the first one, the main parameter is whether the attacker belongs to the network or not, which specifies the intern and the extern attacks. The intern attacks are the most challenged because existing solutions proposed for the extern attacks are not applicable here. The second classification includes active and passive attacks. Here, the active attacks attempt only to monitor and analyze the network traffic and make in danger the confidentiality service. The passive attacks execute actions like modification, injection, or damage of messages. It aim to disturb the correct operation of the network and target availability, integrity, authentication, or non-repudiation services. Other attack classes have existed in the literature which are present with the VANETs networks. Authors in [13] define Malicious vs. Rational attackers, Local vs. Extended attackers, and Independent vs. Colluding attackers. The former category determines the benefit of the adversary while executing an attack in the network. Rational to seek personal benefit, else the attacker is malicious. The second category is based on the area focused by the attacker: local for a limited area and extended for a large scoop. The last category includes the cooperation between adversaries to execute an attack: One attacker and no cooperation define independent attackers in the different cases the attackers are colluding. MANET, VANET, and FANET are vulnerable to many attacks. The medium used in such networks helps attackers to penetrate the networks, thus cause problems like seize control, sabotage the mission on the network or just capture sensitive data. In the literature, many studies have classified the Ad-hoc security attacks into categories [14][15][16]as explained in the following:

Sniffing attacks : A sniffing attack is also known as an eavesdropping or snooping attack. The wireless AdHoc networks are prone to such attacks due to their specific features like the shared wireless medium [14]. Some studies in the literature have classified the sniffing attack as a passive or an active attack [15][16]. The main objective of a malicious node or an attacker is to target personal or sensitive data transmitted between nodes to grab confidential information. Reaching these objectives with a passive attack means just listening to the transited messages during the wireless transmissions. In an active attack, the

attacker sends some queries to the target nodes to build a friendly relationship and exchange information.

Modification attacks : Modification attacks affect the integrity of the messages in the network. Some of these attacks are based on changing the routing packets by using different methods as needed. The self-organized nodes in AdHoc networks make the routing messages in danger face to attackers. Indeed, these malicious nodes apply packets misrouting by changing some routing information like the sequence number, the count hops, or the source node. A different scenario of modification attacks is called a spoofing attack [17]. Here, the attacker falsifies its real identity to create some weakness in the networks. Executing such an attack is based on different methods like changing the IP or the MAC addresses.

Fabrication attacks : Similar to the modification attacks, the fabrication attacks aim at the routing messages [18]. However, in this case, attackers do not modify the existing packets; they create their ones and damage the network services. This category includes attacks that generate false route error messages. Thus, destruct valid routes and cause a denial of service or sleep deprivation. Other attacks under this category exist in state-of-the-art like Rushing Attacks, Wormhole Attacks, and Gray Hole Attack, which will be described further with more details.

Selfish behavior attacks : Nodes in AdHoc mode need to cooperate to ensure the operation of the network [19]. Some nodes in (MANET, VANET, and FANET) are uncooperative due to selfish reasons. Consequently, some important tasks like rooting are not correctly performed. The selfish behavior stops or slows the traffics at the malicious node, which can interrupt the operation of the whole network.

Routing attacks : Routing is a service to find routes for exchanging data between sources and destinations. This process is ensured using routing protocols that have been designed depending on the network characteristics and constraints. Given the importance of this service, many routing protocols have suffered from various attacks, and searches have explored different challenges in this area.

5 Potential attacks and threats on MANET VANET and FANET

5.1 Attacks on MANET

Mobile AdHoc Networks (MANETs) are vulnerable to numerous attacks [19][20][21]. Table 2 briefly describes some exiting attacks by focusing on their types, the affected layer of the OSI model, and the targeted security services.

Table 2 Different type of attacks on MANETs

Attacks	Concepts	Types	Layers	Services
Eavesdropping	Capture and extract sensitive and personal information (data and routing packets)	Passive or Active	Network	Authentication
Jamming attack	-Injection of noisy signals at the physical layer and affect communication -Leads to a denial of service	-Active - External	Physical	Availability Service integrity
Collision attack	-Injection of false control messages in parallel times with other transmissions to make a collision and drop messages -Leads to a denial of service	-Active - External	Link	Availability Data integrity
-Wormhole -Blackhole -Greyhole	-Modifying routes and pretend node to have the optimal route -Redirecting the network traffic through particular links -Collecting, modifying, or deleting data -Leads to a denial of service	-Active	Network	Availability Data integrity Authentication
Routing (Table Overflow, Table Poisoning, Replication, Rushing... etc.)	-Attacks against the routing protocols implemented in the networks -Creating false routes, sending pretended updates, replicating expired packets, etc. -Prevent creating routes, isolating some parts of the network, height consummation in bandwidth, and power energy	-Active	Network	Availability Data integrity
Sybil	-Duplicating the malicious node with multiple identities of nonexistent nodes -Affecting the cooperation between nodes -Leads to a denial of service	Active	Network	Availability Service integrity
IPspoofing	-Impersonation of identity using falsified IP addresses - Denying services and avoid locating the source of the attack -Making a trust relationship between two nodes to take control of one of them	Active	Network	Availability Service integrity Non repudiation
State pollution	-Falsifying parameters in replay -allocating an occupied IP address to new nodes -Flooding the network by a broadcast of duplication address detection messages	Active	Network	Availability Data integrity
SYN Flooding	-Sending many SYN requests for establishing connections with a victim node	Active	Transport	Availability

5.2 Attacks on VANET

Vehicles AdHoc Networks (VANETs) security has received several attentions from researchers and industry [10]. VANETs security aims to provide safety applications that manage road traffic and avoid the loss of human life. VANETs are a subset of mobile ad hoc networks; thus, tab.2 describes some common attacks encountered in VANET and those examined in [13] [22][23]:

Table 3 Different type of attacks on VANETs

Attacks	Concepts	Attacker	Services
-Denial of service (DoS) - Distributed DoS	Many artificial massages in successive transmission by one (DoS) or a group of attackers (Distributed DoS)for flooding and jamming the network	-DoS: Outsider, Active, Local, Independent -Distributed DoS: Insider, Active, Colluding	Availability
-Blackhole	-Area with no participating node in communication -Loss of messages and data packets	-Passive, Outsider	Availability
-GPS Spoofing	-Giving neighbor nodes false information of locations to fake positions	- Active, Insider, Independent	Authentication
-Sybil attack	-Multiple identities for one attacker -Illusion nodes by multiple messages transmitted from different sources	- Insider, Active, Local	Authentication
-Illusion attack	-An application to fabricate message using a voluntarily placed sensor -Transmitting false traffic information	- Insider, Malicious	Data integrity Data trust
-Greedy drivers	-Using the network resources for the own benefit of the attackers -Altering traffic information and jamming the network by false massages to deviate another node from the road	-Insider, Rational, Active	Data integrity
-Timing	-Delaying messages and do not transmit critical information to neighbors in real-time leading to fatal consequences	-Insider, Rational	Data integrity
-Wormhole -	-Two attackers are positioned in the most vital place in the network and create a band wormhole (tunnel). -Intercepting communications and tunneling packets from one location to other vehicles in different locations.	-Insider, Extended, Passive, Colluding	Authentication, Confidentiality

5.3 Attacks on FANET

Flaying AdHoc Networks (FANETs) are also a subclass of mobile ad hoc networks networks, where the need for security is highlighted as a crucial aspect. Indeed, FANETs hold all the classical security issues previously discussed and designs new problems. Table 4 lists the potential attacks targeting the stability of the network services in FANETs [11][24][25].

Table 4 Different type of attacks on FANETs

Attacks	Concepts	Attacker	Services
-Denial of service	-Making the network resources unavailable, so paralyzing the network services	-Internal or external -Active	-Availability
-GPS Jamming	-harm on the navigation to prevent the correct supervision of location, routes, altitude, and direction -Losing the fly control	-External	
-Worm hole	-Recording packets from a vital place in the network -Tunneling the gathered packets to another place to retransmit them	-Internal	-Availability
-Sinkhole	-The attacker broadcast false routing information to attract all the network traffic	-Internal	-Availability
-Power-consuming	-Initiating a big volume of data in the network to make reacting all the network nodes	-External	-Availability
-Man in the middle	-The attacker places itself between the UAV and its Ground Control Station to capturing data from their communication link	-External	-Integrity
-Rooting loop - Integrity	-Modifying the routing information to prevent nodes from finding the valid routes	-External	-Availability
-Malware Software	-Injecting malware like a backdoor in the internal navigation system of UAVs and the control station. -Automatically accept commands by the attacker to take control or pull sensitive data.	-External	-Internal -Integrity -Availability -Privacy

6 Conclusion

The self-organized AdHoc system is the new network generation that offers very significant applications for users. Their specific features like the dynamic topology, the self-configuring nodes, and the wireless communications make the end users or the whole network prone to different attacks. In this paper, we interest in MANET, VANET, and FANET as important real-life examples

of the AdHoc network. The paper introduces the concept of each network and presents the security requirements with the existing attacks. By the end of this review, searchers must invest in ad-hoc network security as a hot topic of search to provide new safety applications and enhance numerous fields. Through the various researches carried out in this area of research, we define our future interests. Our attention will be centered on finding solutions for specific attacks by using and combining methods newly introduced in the literature.

References

1. Ganesan, S and Loganathan, B, A Survey of Ad-Hoc Network: A Survey, International Journal of Computer Trends and Technology (IJCTT), Volume 4, (2013)
2. Student, VRP and Dhir, Renu, A study of ad-hoc network: A review, International Journal, Volume 3, 3 (2013)
3. Belding-Royer, Elizabeth M and Basagni, S and Conti, M and Giordano, S and Stojmenovic, I, Routing approaches in mobile ad hoc networks, 275–300. Wiley Online Library, (2004)
4. Zeadally, Sherali and Hunt, Ray and Chen, Yuh-Shyan and Irwin, Angela and Hassan, Aamir, Book title, page numbers. Publisher, place (year)
5. Bekmezci, Ilker and Sahingoz, Ozgur Koray and Temel, Ş, Flying ad-hoc networks (FANETs): A survey, Ad Hoc Networks, Volume 11, 1254–1270(2013)
6. Zhou, Lidong and Haas, Zygmunt J, Securing ad hoc networks, IEEE network, Volume13, 24–30 (1999)
7. Loo, Jonathan and Mauri, Jaime Lloret and Ortiz, Jesus Hamilton, Mobile ad hoc networks: current status and future trends, 241. CRC Press, (2016)
8. Liu, Gao and Yan, Zheng and Pedrycz, Witold, Data collection for attack detection and security measurement in mobile ad hoc networks: A survey, Journal of Network and Computer Applications, Volume105, 105–122 (2018)
9. Abdel-Fattah, Farhan and Farhan, Khalid A and Al-Tarawneh, Feras H and AlTamimi, Fadel, Security challenges and attacks in dynamic mobile ad hoc networks MANETs, IEEE jordan international joint conference on electrical engineering and information technology (JEEIT), 28–33 (2019)
10. Kumar, Ajay and Bansal, Manu and others, A review on VANET security attacks and their countermeasure, 4th international conference on signal processing, computing and control (ISPCC), 580–585 (2017)
11. Singh, Kuldeep and Verma, Anil Kumar and Aggarwal, Palvi, Analysis of various trust computation methods: a step toward secure FANETs, Computer and cyber security: principles, algorithm, applications, and perspectives, 171–194(2018)
12. Di Pietro, Roberto and Guarino, Stefano and Verde, Nino Vincenzo and Domingo-Ferrer, Josep, Security in wireless ad-hoc networks–a survey, Security in wireless ad-hoc networks–a survey, Volume 51, 1–20 (2014)
13. Malhi, Avleen Kaur and Batra, Shalini and Pannu, Husanbir Singh, Security of vehicular ad-hoc networks: A comprehensive survey, Computers and Security, Volume 89, 101664(2020)
14. La Polla, Mariantonietta and Martinelli, Fabio and Sgandurra, Daniele, A survey on security for mobile devices, IEEE communications surveys and tutorials, Volume1, 446–471 (2012)
15. Anand, Madhukar and Ives, Zachary and Lee, Insup, Quantifying eavesdropping vulnerability in sensor networks, Proceedings of the 2nd international workshop on Data management for sensor networks, 3–9 (2005)
16. Wang, Qiu and Dai, Hong-Ning and Zhao, Qinglin, Eavesdropping security in wireless ad hoc networks with directional antennas, 22nd Wireless and Optical Communication Conference, 687–692 (2013)

17. Al-shareeda, Mahmood A and Anbar, Mohammed and Manickam, Selvakumar and Hasbullah, Iznan H, Review of prevention schemes for modification attack in vehicular ad hoc networks, International Journal of Engineering and Management Research, Volume 10, (2020)
18. Sbai, Oussama and Elboukhari, Mohamed, Proceedings of the 4th International Conference on Smart City Applications, 1–5. (2019)
Author, Book title, page numbers. Publisher, place (year)
19. Rajesh, M, A review on excellence analysis of relationship spur advance in wireless ad hoc networks, International Journal of Pure and Applied Mathematics, Volume118, 407–412 (2018)
20. Abdel-Fattah, Farhan and Farhan, Khalid A and Al-Tarawneh, Feras H and AlTamimi, Fadel, IEEE jordan international joint conference on electrical engineering and information technology (JEEIT), 28–33. IEEE, (2019)
21. Meddeb, Rahma and Triki, Bayrem and Jemili, Farah and Korbaa, Ouajdi, International Conference on Engineering and MIS (ICEMIS), 1–7. IEEE, (2017)
22. Hezam, Mohammed Ali and Junaid, Al and Syed, AA and Nazri, Mohd and Warip, Mohd and Fazira, Ku Nurul and Azir, Ku and Nurul Hidayah, Romli, Classification of security attacks in VANET: A review of requirements and perspectives, EDP Sciences, (2018)
23. Saggi, MK and Sandhu, RK, International Conference on Research and Innovations in Engineering and Technology (ICRIET 2014), 19–20. (2014)
24. Bekmezci, İlker and Şentürk, Eren and Türker, Tolgahan, Security issues in flying adhoc networks (FANETS), Journal of Aeronautics and Space Technologies, Volume 9, 13–21 (2016)
25. Sumra, Irshad and Sellappan, P and Abdullah, Azween and Ali, Ahmad, Security issues and challenges in Manet-Vanet-Fanet: A Survey, EAI Endorsed Transactions on Energy Web, Volume 5, 17 (2018)