EAI Endorsed Transactions
on Energy Web and Information Technologies
Research Article EAI.EU

Security issues and Challenges in MANET-VANET-FANET: A Survey

Irshad Ahmed Sumra[1,*], P. Sellappan[1], Azween Abdullah[2] and Ahmad Ali[3]

[1]Department of Information Technology, Malaysia University of Science and Technology (MUST), Malaysia.
[2]School of Computing and IT, Taylor's University, Subang Jaya, Malaysia.
[3] School of Electronics and Information Engineering, Hebei University of Technology, Tianjin 300401, China.

Abstract

Security is one of the key important factors in ad hoc network due to the open wireless medium and dynamic topology of the network. MANET, VANET and FANET are type of ad hoc network and their applications are served the end users in real environment. VANET and FANET are next generation network and due to safety applications more attractions for end users in these networks. In this paper, we will provide the survey on security issues and challenges in the field of MANET, VANET and FANET. The successful implementation of these networks in real environment, it is require the network will be secure and end user can take benefit from their life safety applications.

Keywords: Security, Mobile ad-hoc network (MANET), Vehicular ad-hoc network (VANET), Flying ad-hoc network (MANET), applications, end user.

Received on 29 November 2017, accepted on 12 February 2018, published on 10 April 2018

doi: 10.4108/eai.10-4-2018.155884

*Corresponding author. Email:isomro28@gmail.com

1. Introduction

Wireless sensor networks (WSNs) are composed of a large number sensor nodes, which are densely deployed over a geographical area. Each node is responsible for getting useful information (e.g. temperature, humidity), and forwards this information to a base station through wireless communication. MANET, VANET and FANET are types of ad hoc network and it is equipped with a number of many embedded sensors nodes and communicates with each other and shares the information from source to destination. Security is one of the key factors for successful implementation of these ad hoc types of network [1]. In modern era of development of computational response, systems may participate in the activity of cybercrime. It may directly destroy and harm any physical system or it may trigger a physical event in which systems give a delay in generating an inceptive vigilance. Many organizations and researchers have been working for many years to protect the security systems against attackers and to minimize the security attacks on the network. Many of the researchers contribute to MANET, VANET and FANET security and proposed many solutions according to the need and situation [2].

The rest of the paper is organized as follows. Section 2 describes the basic security requirement with respect to ad hoc network and their types. Basic concepts of MANET, VANET and FANET with their architecture are discussed in Section 3. Section 4 describes in detail the security issues and challenges in the field of MANET, VANET and FANET and at this level just discuss the security threats and their solutions are not part of this paper. Section 5 is conclusion the survey paper.

2. Basic Security Requirements

The basic security requirements are given below [18]:-

- **Availability**: Nodes should maintain capability its ability to deliver all the designed services not considering of its security state the safety area desecrated during the denial services attack and every authorizes node assess the data [3].

- **Authentication**: Authentication proves the trustable communication between two difference nodes. Identity of the source node is ensure therefore the necessary participant ensure your identity. One way to offer this service is using certifications, who ever in absence of central control unit, key allocation and key management are challengeable.
- **Data confidentially**: Each node or each application specifies the services and permission to access. In MANET as there is no central management, key distribution faced lots of challenges and in some cases impossible.
- **Integrity**: when messages are transmit than integrity grantee identity in MANET**,** according to integrity security service, just authorized nodes can create editor delete packets.
- **Authorization**: In authorization process generally use to allocate different access rights to different intensity of users.
- **Privacy**: Privacy keeps the personal information of the node not scattered by the node itself or the system software, that is, contact is unknown.

3. Basic Concept of MANET-VANET-FANET

3.1 Basic Concept of MANET

Mobile ad-hoc network (MANET) is a collection of wireless nodes that are interconnected each other and dynamically setup anyplace or anytime exclusive of having the pre-existence transportation. There are two variations mobile network: infrastructure and substructure small network [1]. In the case of Infrastructure network mobile communicate through the base station that are connected to fixed infrastructure and the infrastructure of less networks is known's as the mobile ad- hoc networks Mobile ad-hoc network correspond to the composite distributed system MANET requisite exceptionally flexible technology without any fixed base station. The security services such as validity, data reliability, safe communication between layers and privacy are extremely mandatory for MANETs [2,3]. MANET contains some general security threats which appearance in both wired and wireless networks with supplementary security attacks distinctive to itself. The Fig 1. shows the basic architecture of MANET.

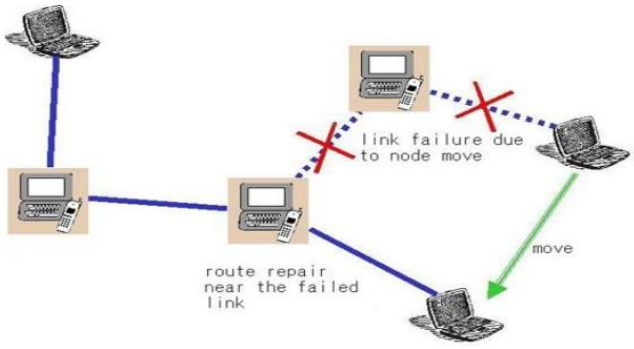

Figure 1. Architecture of Mobile ad-hoc Network (MANET) [2]

3.2 Basic Concept of VANET

Recent year's transportation issues and traffic activities are play vital role in daily life upbringing. So, increase the level of improvement is most important to the growing the better vehicle system [4]. Due to huge amount of traffic and the other side significantly increases the level of accident. Novel technologies have been investigate connecting to the Vehicular Ad Hoc Network (VANET) due to enhancement in vehicular traffic/overcrowding around us [5]. VANET is a basically development system that increase the traffic safety and reduce the road accidents. VANET is a wireless technology that moves the car through the nodes and transfers the messages one node to another node. Node are communicating single hop multi hop and also provide the huge range of network to capture the signals and send the messages. Defiantly, VANET technology enhances the security and traffic transportation [6].Vehicular communication is involved of the nearby vehicles and the appropriate design of VANET to provide the better safety driving. According to the Nazish [7] VANET has the following type of communication ,Inter-Vehicular or Vehicle to Vehicle (V-V) Communication, Vehicle to Roadside or Vehicle to Infrastructure (VI) Communication and Inter Roadside Communication therefore VANET provide the complete computing environment facilitate various services through a assortment of applications. The Fig 2. shows the basic architecture of VANET.

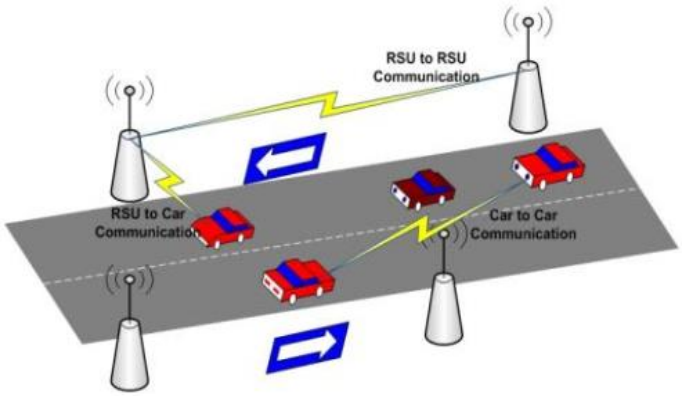

Figure 2. Architecture of Vehicular ad-hoc network (VANET) [5]

3.3 Basic Concept of FANET

Rapid technology advances on electronic device and communication technologies, it has been probable to construct unmanned aerial vehicle (UAV) system, which can fly separately or can be manage slightly [10]. The small operating experience (adaptability, elasticity and easy equipment) usage of UAV assures the modern methods both military and civilian applications. Maintain the communication links between the unmanned aerial vehicles basically in FANET UAV is a demanding task. The topology of these networks is additional forceful than that of distinctive mobile ad hoc networks (MANETs) and of representative vehicle ad hoc networks (VANETs). FANET especially case of MANET attribute and the high degree mobility. The FANET topology change more frequently, when the ordinary infrastructure is out of service or not available [11]. The major essential component routing in FANET bandwidth play the critical role in the process of large amount of data routing decision. One of the major anxieties in FANET is to evade the crash [2]. The Fig 3. shows the basic architecture of FANET and Fig.4 show the comparative architecture overview of types of ad hoc networks(MANET,VANET,FANET).

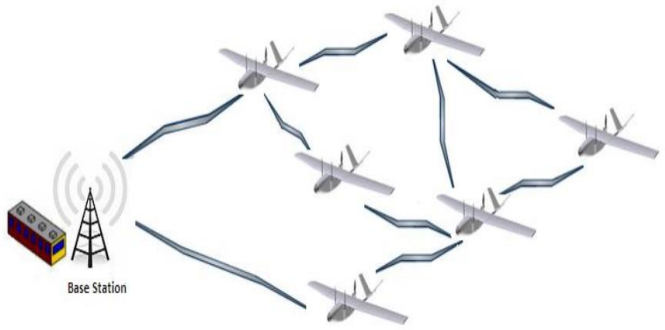

Figure 3. Architecture of Flying ad-hoc network (FANET) [11]

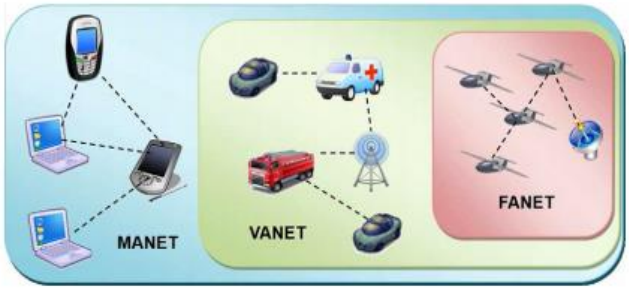

Figure 4. Architecture of MANET, VANET and FANET [10]

4 Security issues and Challenges

4.1 Security issues and Challenges in MANET

The Security issues and challenges in MANET are given below:-

- **Active Attacks:** Active Attack achieves the attacker for duplicate; transform and removal of exchange also try to modify the behavior of protocol. A number of times identify the active attack however active attack fewer used by an attacker. Basically active attack modifies the data packets, inject the packet and drop the packet [2].
- **Passive Attacks:** Passive attack is difficult to be identifying. Routing packet and attacker may understand about a node [12]. Passive attack objective the privacy characteristic of network and complete for distinguish the communication prototype among nodes.

Physical Layer Attacks [12]

1) **Snooping:** In snooping attack, attacker stabs to catch the top-secret information through communication.
2) **Jamming:** Jamming attack will be executed by knowing the incidence malevolent nodes sends jam signal to interrupt the communication.
3) **Active Interfering**: An active prying is a type of denial of service attack which alters the infrastructures.

Link Layer Attacks

1) **Egotistic Misbehaviour of Nodes**: In the egotistical misbehaviour nodes will achieve as selfish and will not be ready to contribute in promote process [12].
2) **DOS Attack:** these attacks avoid official access of capitals to the realistic node [12].

3) **Resource Collapse:** Malicious nodes concept frequent collision to consume the battery power [12].

Network Layer Attacks [12]

1) **Black Hole Attack:** In the Black Hole Attack the attacker node encourage shortest route destination malevolent node can descent packet or achieve DOS attack or Man in the central attack. Malicious nodes inserts fault routing information to the network and guide the packets in the direction of it.
2) **Wormhole Attack:** In this attack two attack involve one attacker delays the packet and other packet passageway and the link of attacker provide high speed communication link between them.
3) **Routing Table Poisoning Attack:** Attacker venoms the routing table by varying the routes in the routing table. Other way is to addition RREQ packet with high arrangement number and low sequence number packet will be deleted. Routing protocols preserve tables that embrace in the sequence concerning routes of the network.

Transport Layer Attacks [12]

Session Hijacking: Here the attacker satires the IP address and launch a variety of attacks using the accurate sequence number and control the session of hijacking.

Application Layer Attacks

1) **Malicious code attacks:** Malicious code attacks both operating system and user application and also includes, Viruses, Worms attack.
2) **Multilayer Attacks:** The DoS attacks, artificial attacks, man-in-the middle attacks, and many other attacks can purpose multiple layers.

4.2 Security issues and Challenges in VANET

The Security issues in VANET are given below [6]:-

Threats to Availability

The threats to availability of vehicle-to-vehicle and vehicle-to-roadside communication are given below [15]:

1) **Denial of Service Attack**: Denial service attack can be complete with approve of indoor and outdoor network. In the cause of VANET produce the artificial messages like Flooding and Jamming.
2) **Broadcast Tampering**: This attack is supported out by an insider. It contributes false safety messages into the VANET to impose damage or detriment to the road users. When attackers influence the traffic on a clear route then accident can happen.
3) **Malware:** This attack is frequently approved by insiders more than outsiders and when a firmware update is done it can be downloaded into the system.
4) **Spamming**: Spam messages in VANET additional problematic to control in VANET because there's no central organization.
5) **Black Hole Attack**: This attack is the cause of broadcasting messages and also nodes declining to contribute in the network when the nodes slump the network than all communications and links had broken.

Threats to Authenticity

In VANET validity requirement is very important. This includes the defending of sensible node from the attackers "inner or outer" insightful the network with false classifies [14,15], such threats are:

1) **Masquerading**: This attack implements the justifiable vehicle in the network and creating of false message and forming of black holes.
2) **Global Positioning System (GPS) Spoofing**: GPS spoofing through the GPS satellite communication creates the false location and move the vehicle wrong side to ensure that this location is right one.
3) **Tunneling:** The attackers rapidly insert false positioning information or data in to the committed unit of the node, origin the node to assume that the information received is valid.
4) **Position Faking**: In blind spot attacker speedy modifies the position and unsecure communication generate the blind spot also dispatch essential and authentic security messages.
5) **Message Tampering:** In this attack, the attacker adjusts and exchanged the message from vehicle-to-vehicle or vehicle-to-roadside unit communication also demand or reply from other nodes.
6) **Message Suppression/Fabrication/Alteration:** The attackers essentially restrain the communication link between vehicles or change the application so that the vehicle cannot send or receive or return to application.

Threats to Confidentiality

Messages that are swapped between nodes (vehicles) in VANET are open to privacy threats or attack with method such as illegal variety of messages during snooping and passive attacks which are confirmed in the journalism by the investigators [15].

Security Challenges in VANET

The Security challenges in VANET are given below:-

- **Real Time Constraints**: VANET achieve the real time constraints so, required the specific timing to deliver the massages. Achieve this goal use very fast cryptographic algorithm.
- **Data consistency Liability**: Data consistency is important in VANET and avoids the unnecessary information because authenticate node execute the malicious.
- **Key Distribution**: VANET use the key to send and receive the messages encrypts the message and after procedure complete decrypt the message that's why

key distribution is an important procedure and perform the major challenge.

- **High mobility**: High mobility is required in VANET nodes are connected each other's and transfer the signals to communicate the other vehicle so very fast mobility level is required. VANET required less execution time.
- **Non- repudiation**: In this procedure node cannot refuse but does not send the messages and signals. [14].
- **Data verification and privacy**: To preserve the integrity, regular bases check the verification and privacy is very essential characteristic in VANET.

4.3 Security issues and Challenges in FANET

The Security issues in VANET are given below [16,17]:-

- **National Regulations:** UAV is used many application areas in FANET. Many countries' present the air regulation does not allow restricted UAV operations in civil airspace.
- **Routing:** Data routing between UAC major challenges the routing conventions should be able to update routing tables animatedly conferring to topology changes, so must require to develop new routing algorithms and networking modals for assemble the flexible Modal.
- **Path Planning:** Path planning is play very vital role in FANET so; acquire new algorithms methods and dynamic path planning is very essential to achieve the goals. Many case each UAV has to change its preceding path, and new ones must be recalculated animatedly.
- **Integration with a Global Information Grid (GIG):** GIG is a universal network system provide intend capabilities that collaborate the each other A FANET should connect further information grid. Grid is one of the main proposals that increase the efficiency of a UAS by using UAV.
- **Coordination of UAVs and manned aircrafts**: UAVs collaborate is necessary to maintain the FANET aircraft network environment is necessary to fulfill the flying requirement the coordination of UAV will allow the destruction of enemy aircraft with negligible losses.
- **Standardize FANETs:** To reduce the frequency obstruction issues need to use standardize communication
- **UAV mobility and placement:** Use different sensors that loaded the different, while another UAV is prepared with a high resolution camera and also allow the several images to be taken from the similar areas.

Security Challenges in FANET

The Security challenges in VANET are given below [11]:-

- **Routing:** In FANET routing is diverse from the other ad hoc network because the node movement is very high and the topology modify very frequently two major challenges are to be shown in routing:
  - Routing algorithm work high mobility
  - Routing algorithm should be quick to update
- **Security:** In FANET mange the secure routing point is: Make sure Confidentiality, Integrity and Availability of precious information in FANET so these networks are essential to mange. Lack of physical security node compromises there is another issue in FANET. Trust management is another important point. In FANET nodes leave and join very frequently [2] Accessibility routing algorithms for ad-hoc networks are unable in the opposition to frequent network topology modify and malicious attacks in FANET.
- **Quality of Service (QOS):** The parameters quality of services able is to be improved. In FANET different type of data are transformed like image, video, audios, text etc.
- **UAV Mobility and Placement:** UAV are the available various capabilities and capacities for different purposes basically the placement of UAV is appropriate the major concern in FANET [2]. Open challenges is to optimize the UAV placement.
- **Scalability:** Perfume more tasks required more UAV because singe UAV can perform restricted task. So, FANET algorithm design should be they can accommodate many UAV.
- **Reliable and Secure data transfer:** FANET application transfers the perceptive information that's why reliability of network is very elevated and defines the significant data. Table I, provides the comparison analysis between MANET,VANET and FANET with different parameters.

Table 1. Comparison different types of ad-hoc networks [11]

Parameters	MANET	VANET	FANET
Mobility	Low	High	Very High
Nodal Density	Low	High	Very Low
Mobility Model	Random	Regular	Random
Topology Change	Slow	Fast	Fast
Line of Sight	Not Available	In Some Cases	Available
Localization	GPS	GPS,AGPS	GPS,AGPS

5 Conclusion

The applications are core component of ad hoc network and basic purpose of these applications to serve the users. The behavior of the nodes in MANET, VANET and FANET are dynamic nature due to different types of topology and network nature. The applications of these networks are directly connect to the end user and security is important milestone to serve the user in dynamic environment. Attackers are also part of this network and it is very difficult to monitor the behavior of attackers and nature of attacks in network. In this survey paper, emphasis various security issues in MANET, VANET and FANET and also discuss in detail the key security challenges in the field of MANET, VANET and FANET. In future work, we will discuss in detail the security solution of security issues and challenges in MANET, VANET and FANET.

References

[1] C. Zhu, C. Zheng, L. Shu, and G. Han, "A survey on coverage and connectivity issues in wireless sensor networks," *Journal of Network and Computer Applications*, vol. 35, no. 2, pp. 619–632, 2012.

[2] R. Nandakumar K. Nirmala "Security Challenges in Mobile Ad Hoc Networks - A Survey" Australian Journal of Basic and Applied Sciences, Vol. 10(1), pp. 654-659, January 2016.

[3] Arun Kumar Yadav Karan Singh "Advanced Research in Computer Science and Software Engineering Evaluation of Security Threats and Solutions in MANET'S" International Journal Volume 6, Issue 2, February 2016

[4] N. Kowsalya, M. Karthika, N. Boomathi "Analytical Study on Security Issues in Mobile Ad-Hoc Network" International Journal of Innovative Research in Computer and Communication Engineering Vol. 4, Issue 6, June 2016.

[5] S. Banu Priya1, C.Theebendra2 "A Study on security challenges in mobile ad hoc network" International journal of research in computer applications and robotics, ISSN 2320-7345 February 2016.

[6] Sumra IA, Bin Hasbullah H, Bin AbManan J. Attacks on security goals (confidentiality, integrity, availability) in VANET: A survey. Vehicular Ad-hoc Networks for Springer. Smart Cities, Advances in Intelligent Systems and Computing; 2015. p. 51–61.

[7] T. Ramaprabha, V. Premalatha,"A survey on security issues and challenges in VANET" International Journal of Contemporary Research in Computer Science and Technology (IJCRCST) e-ISSN: 2395-5325 Volume2, Issue 7 (July '2016).

[8] Khan, F., ur Rehman, A., Usman, M., Tan, Z., & Puthal, D. (2018). Performance of Cognitive Radio Sensor Networks Using Hybrid Automatic Repeat ReQuest: Stop-and-Wait. Mobile Networks and Applications, 1-10.

[9] Yousef Al-Raba'nah, Ghassan Samara, "Security Issues in Vehicular Ad Hoc Networks (VANET): a survey", International Journal of Sciences & Applied Research (IJSAR), 2(4), 2015; 50-55.

[10] Khuldeep Kumar,Sandeep Kumar Arrora "Review of Vehicles Ad HocNetwork Security" International Journal of Grid and Distributed Computing Vol. 9, No. 11 (2016).

[11] Fida, N., Khan, F., Jan, M. A., & Khan, Z. (2016, September). Performance Analysis of Vehicular Adhoc Network Using Different Highway Traffic Scenarios in Cloud Computing. In International Conference on Future Intelligent Vehicular Technologies (pp. 157-166). Springer.

[12] Kuldeep Singh "A Secure Framework for Flying Ad-hoc Networks"http://phd.medialabasia.in/userdata/docs/1631_Synopsis.pdf

[13] Shashank Kumar Singh "A Comprehensive Survey on Fanet: Challenges and Advancements" International Journal of Computer Science and Information Technologies, Vol. 6 (3) , 2015, 2010-2013.

[14] Nabeel Zanoon1, Nashat Albdour2, Hatem S. A. Hamatta1, and RashaMoh'd "Security challenges as a factor affecting the security of MANET :attacks and security solutions",International Journal of Network Security & Its Applications (IJNSA) Vol.7, No.3, May 2015.

[15] Jan, M. A., Khan, F., Alam, M., & Usman, M. (2017). A payload-based mutual authentication scheme for Internet of Things. Future Generation Computer Systems.

[16] Felipe Domingos da Cunha, Azzedine Boukerche, Leandro Villas, Aline Carneiro Viana, Antonio A. F. Loureiro "Data Communication in VANETs: A Survey, Challenges and Applications" https://hal.inria.fr/hal-00981126/PDF/RR-8498.pdf march 2014.

[17] Naveen , Sunil Maakar M.Tech Scholar "Concept of Flying Ad-hoc Network: A Survey" National Conference on Innovative Trends in Computer Science Engineering (ITCSE-2015) held at BRCMCET, Bahal on 4th April 2015.

[18] Sumra, Irshad Ahmed; Ahmad, Iftikhar; Hasbullah, Halabi; bin Ab Manan, Jamalul-lail; , Behavior of attacker and some new possible attacks in Vehicular Ad hoc Network (VANET), Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2011 3rd International Congress on , vol., no., pp.1-8, 5-7 Oct. 2011.

[19] Sumra IA, Bin Hasbullah H, Bin AbManan J. Attacks on security goals (confidentiality, integrity, availability) in VANET: A survey. Vehicular Ad-hoc Networks for Springer. Smart Cities, Advances in Intelligent Systems and Computing; 2015. p. 51–61.