IJCSE International Journal of Computer Sciences and Engineering Open Access
Survey Paper Vol.-6, Issue-11, Nov 2018 E-ISSN: 2347-2693

A Survey on Vulnerabilities, Attacks and Issues in MANET, WSN and VANET

R. Yogapriya[1*], A. Subramani[2]

[1]Dept. of Computer Science,M.V.Muthiah Govt. Arts College for Women, Dindigul,Tamilnadu, India - 624001.
[2]Dept. of Computer Science, M.V. Muthiah Govt. Arts College for Women, Dindigul, Tamilnadu, India - 624001.

*Corresponding Author:yogapriya994@gmail.com

Available online at: www.ijcseonline.org

Accepted: 25/Nov/2018, Published: 30/Nov/2018

***Abstract*—** An attack in computers systems and its networks may attempt to explore, disable, destroy, steal or gain unauthorized access to make illegal use of asset. World Economic Forum has observed that Scalable algorithms and Robustness of cyber-attacks have significant improvement in the technology. Recent technical reports stated that offensive cyber capabilities were developed more rapidly than our ability to deal with hostile incidents. A computer network attack disrupts the integrity or authenticity of data, usually through malicious code that alters program logic that controls data, leading to errors in output. Network security covers a wide variety of both public and private networks that are regularly utilized in jobs like, transactions and communications among businesses, government agencies and individuals. The review paper presents about the types of attacks with issues and challenges in MANET, WSN and VANET.

Keywords: MANET, WSN, VANET, Security, Attacks, Vulnerabilities.

I. INTRODUCTION

MANET: Mobile Adhoc Network (MANET) may be a kind of ad hoc network that may amendment locations and assemble itself on the fly. As a result of MANET's area unit mobile, they use wireless connections to attach to various networks. This will be a typical Wi-Fi association, or another medium, like a cellular or satellite transmission. Some MANETs area unit restricted to a neighborhood area of wireless devices (such as a bunch of portable computer computers), whereas others is also connected to the net. For instance, A VANET (Vehicular ad hoc Network), may be a kind of MANET that permits vehicles to speak with wayside instrumentation. Whereas the vehicles might not have an immediate net association, the wireless wayside instrumentation is also connected to the net, permitting knowledge from the vehicles to be sent over the net. The vehicle knowledge is also accustomed live traffic conditions or keeps track of hauling fleets. Attributable to the dynamic nature of MANETs, they're generally not terribly secure, thus it's vital to use caution what knowledge is shipped over a MANET.

WSN: Wireless sensor Network (WSN) refers to a bunch of spatially spread and dedicated sensors for observation and recording the physical conditions of the setting and organizing the collected information at a central location. WSNs live environmental conditions like temperature, sound, pollution levels, humidity, wind, and so on. WSNs are spatially distributed autonomous sensors to observe physical or environmental conditions, like temperature, sound, pressure, etc. and to hand and glove pass their information through the network to a main location. The additional fashionable networks are bi-directional, conjointly sanctionative control of sensor activity. The event of wireless detector networks was driven by military applications like parcel of land surveillance; these days such networks are employed in several industrial and shopper applications.

The WSN is constructed of "nodes" from some to many lots of or maybe thousands, wherever every node is connected to at least one detector. Every such detector network node has generally many parts: a radio transceiver with an enclosed Antenna or affiliation to an external antenna, a microcontroller, and an electronic circuit for interfacing with the sensors and an energy supply, sometimes electric battery or AN embedded kind of energy harvest home. A detector node would possibly vary in size from that of a shoebox all the way down to the dimensions of a grain of dirt, though functioning "motes" of real microscopic dimensions have however to be created. The value of detector nodes is equally variable, starting from some to many bucks, looking on the quality of the individual detector nodes. Size and value constraints on detector nodes end in corresponding

constraints on resources like energy, memory, machine speed and communications information measure.

VANET: Vehicular Adhoc Networks (VANETs) area unit created by applying the principles of mobile ad hoc networks the spontaneous creation of a wireless network for Vehicle-to-Vehicle (V2V) information exchange to the domain of vehicles. VANETs were 1st mentioned and introduced in 2001 below "car-to-car unintentional mobile communication and networking" applications, wherever networks are often shaped and knowledge are often relayed among cars. It absolutely was shown that vehicle-to-vehicle and vehicle-to-roadside communications architectures can co-exist in VANETs to supply road safety, navigation, and alternative wayside services. VANETs area unit a key a part of the intelligent transportation systems (ITS) framework. Sometimes, VANETs area unit referred as intelligent transportation networks. While, within the early 2000s, VANETs were seen as a mere matched application of MANET principles, they need since then developed into a field of analysis in their title. By 2015, the term VANET became principally similar with the a lot of generic term Inter-Vehicle Communication (IVC), though the main focus remains on the facet of spontaneous networking, a lot of less on the utilization of infrastructure like Road facet Units (RSUs) or cellular networks.

II. TYPES OF ATTACKS

An attack is an information security threat that involves an attempt to obtain, alter, destroy, remove, implant or reveal information without authorized access or permission. It happens to both individuals and organizations. There are many different kinds of attacks, including but not limited to passive, active, targeted, click jacking, brand jacking, botnet, phishing and spamming, etc.

Table 1. Types of Attacks

Active Attacks	**Spoofing Modification Wormhole Fabrication Denial of Services Sinkhole Sybil**
Passive Attacks	**Traffic analysis Eavesdropping Monitoring**
Advance Attacks	**Black hole Attack Rushing attack Replay attack Byzantine attack Location disclosure attack**

Active Attack: Active attacks are attacks, which make some modification in the original message or creation of some false message. These attacks are very complex and cannot prevent easily [1].

Spoofing: In the spoof attack, the hacker modifies the source address of the packets he or she is sending so that they appear to be coming from someone else. This may be an attempt to bypass your firewall rules [5].

Modification: When malicious node performs some modification in the routing route, so that sender sends the message throughthe long route. This attack cause communication delay occurred between sender and receiver [1].

Wormhole: This attack is also called the tunneling attack. In this attack, an attacker receives a packet at one point and tunnels itto another malicious node in the network. So that a beginner assumes that he found the shortest path in the network [2].

Fabrication: A malicious node generates the false routing message. This means it generate the incorrect information about theroute between devices [3].

Denial of services: In denial of services attack, malicious node sending the message to the node and consume the bandwidth of thenetwork. The main aim of the malicious node is to be busy the network node. If a message from unauthenticatednode will come, then receiver will not receive that message because he is busy and beginner has to wait for thereceiver response [1].

Sinkhole: Sinkhole is a service attack that prevents the base station from obtaining complete and correct information. In thisattack, a node tries to attract the data to it from his all-neighboring node. Selective modification, forwarding, dropping of data can be done by using this attack [2].

Sybil: The Sybil attack refers to represent multiple identities for malicious intent. This can be achieved if the malicious nodes collude and share their secret keys [4].

Passive Attack: A passive attack monitors unencrypted traffic and looks for clear-text passwords and sensitive information that can be used in other types of attacks. The monitoring and listening of the communication channel by unauthorized attackers are known as passive attack [5].

Traffic analysis: In the traffic analysis attack, an attacker tries to sense the communication path between the sender and receiver. An attacker can found the amount of data, which is travel from the route of sender and receiver. There is no modification in data by the traffic analysis [1].

Eavesdropping: Eavesdropping is a passive attack, which occurred in the mobile ad-hoc network. The aim of eavesdropping is to find some secret or confidential information that should be kept secret during the communication. This confidential information may be privet or public key of sender or receiver or any password. [7].

Monitoring: In this attack in which attacker can read the confidential data, but he cannot edit the data or cannot modify the data [1].

Advance Attacks:
Black hole: In a black hole attack a malicious node injects false route replies to the route requests it receives advertising itself as having the shortest path to a destination [6].

Rushing attack: In rushing attack, an attacker comes between the route of sender and receiver. When sender send packet to the receiver, then attacker intercept the packet and forward to receiver. Attacker performs duplicate suppression mechanism and then sends the duplicate to the receiver repeatedly. Receiver assumes that packets come from sender so that receiver will be busy continuously. This way, it reduces the efficiency of receiver [7].

Replay attack: It is a network attack in which a malicious node may repeat the data or delayed the data. Originator who intercept the data and retransmit it can do this. Suppose node S want to send some data to R. For this S has to prove his identity to R. This way S sends his password to R for identification. At that time, an attacker an intercept the password of S and a presenting itself as S, when asked for the proof of identity. A sends S password read from the last session, which R accepts [7].

Byzantine Attack: In this attack, a compromised intermediate node or a set of compromised intermediate nodes works in collusion and carries out attacks such as creating routing loops, forwarding packets on non-optimal paths and selectively dropping packet, which results in disruption or degradation of the routing services. It is hard to detect byzantine failures. [7].

Location disclosure attack: Malicious node collects the information about the node and about the route by computing and monitoring thetraffic. This way malicious node may perform more attack on the network [7].

Year-Wise Attacks Report:
The listed below table mentioned that, the types of attacks and its affected percentage in various field are detected in year wise. The below table of 2015 table explain the top attacks affected the network field on that year and its effects are calculated as percentage as a report. The below table on attacks in 2016 is based on a chart from the 2016 McAfee Labs Threat Report. It highlights the top network attack types in 2015, based on data from millions of sensors across file, web, message, and network vector. The top network attacks on the year 2017 recorded from April to June 2017, and published in the Sept. 2017 Quarterly Threat Report from McAfee Labs.

Table 2.Year-Wise Attack Reports

Year	Attacks	Percentage
2015	Denial of service attacks	37%
	Brute Force Attacks	25%
	Browser Attacks	9%
	Shell Shock Attacks	7%
	SSL attacks	6%
	Backdoor attacks	2%
	Botnet Attacks	2%
2016	Browser Attacks	36%
	Brute Force Attacks	19%
	Denial of service attacks	16%
	SSL attacks	11%
	DNS attacks	3%
	Backdoor attacks	3%
	Browser Attacks	20%
2017	Brute Force Attacks	20%
	Worm Attacks	13%
	Malware Attacks	10%
	Web Attacks	4%
	Other Attacks	14%

III. VULNERABILITIES

Vulnerabilities in VANET: VANET is mainly aimed at providing safety related information and traffic management. Safety and traffic management entails real time information and directly affect lives of people travelling on the road.

Simplicity and security of VANET mechanism ensures greater efficiency. VANET builds a robust Ad-Hoc network between mobile vehicles and roadside units. It is a form of MANET that establishes communication among nearby vehicles and adjacent fixed apparatus, usually described as roadside apparatus [8].

VANET architecture is vulnerable to unauthorized access, illegal use, eavesdropping, protocol tunneling, etc. Author Tyagi P, Dembla D, editors of "Investigating the security threats in Vehicular ad hoc Networks (VANETs)" give a comprehensive investigation and discussion on VANET vulnerabilities and Attacks and they classify VANET attacks into many categories [9]. The severity of attacks launched bythe attackers can vary based on the motive of the attack and the potential impact on the victim.

Some VANET Vulnerabilities are:

- Jamming
- Forgery
- Impersonation
- Privacy

VANET was initially intended to integrate mobile connectivity amongst vehicles to expedite data transfer while traveling; vehicles in VANET have been victims to viruses, forged messages, phishing, identity thefts and manyother threats. An issue of paramount concern in vehicular environment is security, where a wrong message may directly affect human life, especially in the light of the public acceptance of the technology.

Vulnerabilities in WSN: Wireless networks have offered attractive flexibility to both network operators and users. Wireless Sensor Networks are vulnerable to various types of attacks. These attacks are mainly of three types : **Attacks on secrecy and authentication**: standard cryptographic techniques can protect the secrecy and authenticity of communication channels from outsider attacks such as eavesdropping, packet replay attacks, and modification or spoofing of packets [10]. **Attacks on network availability**: attacks on availability of WSN are often referred to as Denial-of-Service (DoS) attacks. **Stealthy attack against service integrity**: in a stealthy attack, the goal of the attacker is to make the network accept a false data value. For example, an attacker compromises a sensor node and injects a false data value through that sensor node. In these attacks, keeping the sensor network available for its intended use is essential. DoS attacks against WSNs may permit real-world damage to the health and safety of people [10].

The existing security mechanisms are inadequate, and new ideas are needed because of the following reasons:

- Energy Limitation
- Deployment in an environment more open to physical attack
- Close interaction with physical environment and with people

Therefore, because of its peculiar nature, the WSN must be secured with more than the traditional computer network security techniques [11].

Vulnerabilities in MANET: Mobile Ad hoc Networks (MANETs) refers the one kind of mobile networks encompasses the wirelessmobile nodes for communication. These nodes organize themselves dynamically in random and volatile topologies.

MANETs are used in the following areas:

- Military Battlefield
- Sensor Networks
- Commercial Sector
- Medical Service
- Personal Area Network

Some Vulnerability in MANET is, **No Secure Boundaries-** In a wired network, adversaries have to get physical access to the network medium. They may evenhave to go through layers of firewall and gateway. But, in MANETs, it is easy to gain access to the network,provided the node is in frequency range. Thus, MANETs do not provide secure boundary[12].

Power and Computational Limitations-Wired networks can get electric power supplies, but in the case of wireless network, there is restrictedpower supply. Thus, any node in a network may act selfish, if it has limited power supply [13].

Lack of Centralized Management Facility-Ad hoc networks do not have a central mechanism that is used for management, leading to somevulnerable problems. The lack of centralized management machinery makes the identification of attacks avery difficult problem as it is not easy to check and control the traffic in a highly dynamic and large-scale adhoc network.

Cooperativeness-The common assumption about routing algorithms in MANETs is that the nodes are cooperative andnon-malicious. Thus, a malicious attacker can easily become an essential routing agent and interrupt networkoperations by disobeying the protocol specifications [12].

A wireless ad-hoc network will not have a clear line of defense, and every node must be prepared for encounters with an adversary directly or indirectly. Applications and services in a mobile wireless network can be a weak link as well. In these networks, there are often proxies and software agents running in base-stations and intermediate nodes to achieve performance gains through caching, content transcending, or traffic shaping, etc [13].

IV. SECURITY ISSUES

Security Issues in MANET:

The security issues in MANETs are more challenging than those in traditional wired computer networks and the Internet. Providing security in sensor networks is even more difficult than in MANETs due to the resource limitations of sensor nodes.

Most sensor networks actively monitor their surroundings, and it is often easy to deduce information other than the data monitored.

The security challenges in MANET are discussed by the authors PriyankaGoyal, VintiParmar, Rahul Rishi, on the paper "MANET: Vulnerabilities, Challenges, Attacks,Applications" [15].

Those are:

- Routing
- Security and Reliability
- Quality of Service (QoS)

- Inter-networking
- Power Consumption

Security Issues in WSN:
Security in sensor networks is complicated by the constrained capabilities of sensor node hardware and the properties of the deployment. Some security complications in WSN are: An attacker can easily inject malicious messages into the wireless network. The use of radio transmission, along with the constraints of small size, low cost, and limited energy, make WSNs more susceptible to denial-of-service attacks. Attacks on a WSN can come from all directions and target at any node leading to leaking of secret information, interfering message, impersonating nodes etc. Other security issues are security-energy assessment, data assurance, survivability, Trust, end-to-end security, Security and Privacy Support for data centric sensor networks (DCS) and node compromise distribution [14].

Security Issues in VANET:
VANET packets contains life critical information hence it is necessary to make sure that these packets are not inserted or modified by the attacker; likewise the liability of drivers should also be established that they inform the traffic environment correctly and within time. These security problems do not similar to general communication network. The size of network, mobility, geographic relevancy etc makes the implementation difficult and distinct from other network security. The security challenges in VANET are:

- Real time Constraint:
- Data Consistency Liability
- Low tolerance for error
- Key Distribution
- Incentives
- High Mobility

Those security challenges are briefly discussed on paper [16].The security of vehicular networks is indispensable, because otherwise the systems could make antisocial and criminal behavior easier, in ways that would actually jeopardize the benefits of their deployment. VANETs must work properly in a wide range of conditions, including sparse and dense vehicular traffic. There is a strong need for adaptive transmit power and rate control to achieve a reasonable degree of reliable and low latency communication. In addition, there is a challenge in balancing security and privacy needs. On the one hand, the receivers want to make sure that they can trust the source of information.

V. CONCLUSION

Finally I conclude that, In Ad-hoc network there is no need of any pre-established infrastructure or centralized administration. Globally it can be utilized anywhere. In particular Mobile Ad-hoc Networks (MANET), Wireless Sensor Networks (WSN), and Vehicular Ad-hoc Networks (VANET) are prominent in the field of Ad-hoc networks because it consumes low energy level. From this survey, we discuss more secure related issues and challenges with numerous vulnerabilities, attacks in MANET, WSN and VANET.

REFERENCES

[1] Mohan V. Pawar, Anuradha "Network Security and Types of Attacks in Network", Procedia Computer Science 48, 503 – 506, 2015.

[2] NehaKhandelwal, Prabhakar.M. Kuldeep Sharma, "An Overview Of security Problems in MANET", ISEM International Conference, 2011.

[3] Anupam Joshi and Wenjia Li. "Security Issues in Mobile Ad Hoc Networks- A Survey", research gate.

[4] Ali Ghaffari, "Vulnerability and Security of Mobile Ad hoc Networks", Proceedings of the 6th WSEAS International Conference on Simulation, Modelling and Optimization, Lisbon, Portugal, 124-130, 2006.

[5] Monali S. Gaigole "The Study of Network Security with Its PenetratingAttacks and Possible Security Mechanisms", International Journal of Computer Science and Mobile Computing, Vol.4 Issue.5, PP: 728-735, 2015.

[6] SarveshTanwar, Prema K.V "Threats & Security Issues in Ad hoc network: A Survey Report", International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, Volume-2, Issue-6, 2013.

[7] Satyam Shrivastava, "A Brief Introduction of Different type of Security Attacks found in Mobile Ad-hoc ",/ International Journal of Computer Science & Engineering Technology (IJCSET), Vol. 4 No. 218-222, 2013.

[8] DivyaChadha, "Vehicular Ad hoc Network (VANETs): A Review"

[9] Tyagi P, DemblaD,"Investigating the security threats in Vehicular ad hoc Networks (VANETs)", proc. IEEE International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2014.

[10] Dr.H.G.Chandrakanth, Rajkumar, Sunitha.K.R "A Survey on Security Attacks in Wireless Sensor Networks", International Journal of Engineering Research and Applications, Vol. 2, Issue 4, 1684-1691, 2012.

[11] V.E.Ekong,"A Survey of Security Vulnerabilities in Wireless Sensor Networks", Nigerian Journal of Technology (NIJOTECH) Vol. 35, No. 2, 392 – 397, 2016.

[12] Sarika SA, PravinAb, Vijayakumar AC, Selvamani KD, "Security Issues In Mobile Ad Hoc Networks"

[13] Yongguang Zhang and Wenke Lee, "Security in Mobile Ad-Hoc Networks", Book Chapter.

[14] T.Kavitha, D.Sridharan, "Security Vulnerabilities In Wireless Sensor Networks: A Survey", Journal of Information Assurance and Security 5, 031-044, 2010.

[15] PriyankaGoyal, VintiParmar, Rahul Rishi, "MANET: Vulnerabilities, Challenges, Attacks, Applications", IJCEM International Journal of Computational Engineering & Management, Vol. 11, 32-38, 2011.

[16] Ram Shringar Raw, "Security Challenges, Issues and Their solutions For VANET", International Journal of Network Security & Its Applications (IJNSA), Vol.5, No.5, 2013.

Authors Profile

Ms.R.Yogapriya, Research Scholar is currently pursuing M.Phil in Department of Computer Science, M.V.Muthiah Government Arts College For Women, Dindigul Affiliated to Mother Teresa university,Kodaikanal.She pursued her Bachelor of Computer Science degree from N.P.R Arts and Science College Natham, Affiliated to Madurai Kamaraj University,Madurai and pursued Master of Computer Applications from P.S.N.A College of Engineering and Technology , Dindigul, Affiliated to Anna University Chennai. Her main area of research focuses on Network Security, Mobile Ad-hoc Networks, Mobile Computing and Computer Networks.

Dr. A. Subramani is currently working as an Assistant Professor, Department of Computer Science, M.V.Muthiah Government Arts College For Women, Dindigul and as a Research Guide in various Universities. He received his Ph.D Degree in Computer Applications from Anna University, Chennai. He is a Reviewer of 10 National/International Journals. He is in the editorial board of 6 International/National Journals. He is an Associate Editor of Journal of Computer Applications. He has published more than 90 technical papers at various National / International Conference and Journals. His area of research includes High Speed Network, Routing Algorithm, Soft Computing, Wireless Communication and Mobile Ad-hoc Networks.

