RESEARCH REVIEW JOURNALS
Volume-04
Issue-03
March -2019

ISSN: 2455-3085 (Online)
RESEARCH REVIEW International Journal of Multidisciplinary
www.rrjournals.com [UGC Listed Journal]

Implementation of the Attack Scenario on Manet

[1]Gurpinder Singh and [2]Vijay Dhir

[1]*Research Scholar,Department of Computer Science Application, Sant Baba Bhag Singh University, Jalandhar,Punjab, India*
[2]*Director, Department of Research & Development, Sant Baba Bhag Singh University, Jalandhar, Punjab, India*

ARTICLE DETAILS

Article History
Published Online: 15 March 2019

Keywords
Developing, Wireless, Devices, MANET, Packet, System, Attack

ABSTRACT

Information Technology is the growing filed which is developing day by day. Various government organizations have a huge capability to utilize difficult situations. MANET is an integration of wireless devices that communicate by posting packets to each other without any regulatory information which can be used for the routing. MANET's deal with many boundless systems and are more versatile to different network systems. They are having insecure packets transmission and correspondence in MANETS is a very big issue because MANET deals with different type of threats which are responsible in packet drops. One of them is Sybil Attack, which is used in the communication module in this paper we proposed attack scenario. To secure such systems, important considerations must be taken to reduce the chances of dropping packets.

1. Introduction

MANET is the self-directed devices connected multi-hop and peer to peer and attitude without the use of any access points and central base stations. Each node has communication abilities and nodes can communicate openly with each other in MANET. All nodes join in routing and the performance is depending upon the behavior among the nodes. MANET's is suitable where installation of infrastructure is not possible. In MANET, each node able to self-creating, self-configuring, self-administrating without install any kind of infrastructure. In this paper, we will discuss various security threats in communications. Communication module is vulnerable to different types of attacks[15]. One of the Ad-hoc network attack is the Sybil attack, where the attacker copies multiple identities of sensor nodes into the network.

2. Manet Applications

Mobile devices are expanding day to day and their progress in wireless communication, MANET organizing and picking up significance with the expanding number of across the board applications. MANET is using in various sectors like business, government and private. MANET permit clients to access and exchange data. all hubs in MANETs are mobile and their clients are dynamic and they don't require a static infrastructure table 1 is showing MANET Application and purpose of using.

Manet Applications	Description
Home and Enterprise networking	Home or office wireless networking (WLAN) use PDA to print documents anywhere with the help of shared whiteboard application. PAN Personal Area Network create with the help of infrared, Bluetooth recently we are using Wi-Fi Connectivity.
Educational applications	Setup ad-hoc communication during conference, meetings or lectures, Set up virtual classrooms.
Commercial environments	Setup ad-hoc operation for video conference during operation of the patient. E-commerce: electronic payment payments from anywhere to any other account by Paytm, google pay, phone pay app mobile bill, home bill, taxi bill. Business: Access to customer database stored in a central location flipcart, amazon Paytm. Vehicular services: Local Ad-hoc network with nearby vehicles for road accidence guidance. Transmission of news, road conditions weather forecasting
Emergency Service	Disaster recovery earthquake, fire flood. Search and rescue operations Supporting doctors and nurses in hospitals for patient monitoring

Table 1 (Application of MANET)

MANET's can be used forrelief efforts, e.g. in fire, flood, or it may be earthquake in emergency or rescue operations. This may be because the area is too remote and all equipment has been destroyed. Rescuers personnel communication in order to make the best user to maintain safety. it will automatically be establishing a data network with the communication equipment that rescuers have already carried with them for their job easier.

3. Manet Security

Security is an important requirement in MANETnetwork compared to wired networks. MANETs are more vulnerable to security attacks due to the lack of a trusted centralized

authority and limited resources. wireless transmission ranges can communicate directly nodes outside each other's range. There are many routing protocols from which any one routing protocol must encapsulate an essential set of security mechanism. These mechanisms are used to prevent, detect and respond to security attacks.

4. Types of attack

There are many types of attacker available in MANETs, which are continue attempts to reduce the performance of networks. We will study about various attackers in this paper which are categorised in the table 2.

Layer		Types of attacks
Application	:	Malicious code, Data corruption, viruses and worms
Transport	:	Session hijacking attack, SYN Flooding attack
Network	:	Blackhole, Gray Hole, wormhole, Sinkhole, Link spoofing, Rushing Attack, Replay attacks, Link Withholding, Resource Consumption Attack, Sybil attack
Data	:	Selfish misbehaviour, malicious behaviour, traffic analysis, ARP Spoofing, MAC Flooding, Port Stealing, DHCP Attacks etc..
Physical	:	Eavesdropping, jamming, activeinterference

Table2 (Attacks of MANET)

(i) Attacks at Physical Layer: -

The physical layer is hardware-oriented, they need the help of hardware resources[1]. Compared with other attacks, these types of attacks are very simple to execute. They do not need complete technical knowledge. There are Some attacks identified at physical layer include eavesdropping, jamming and interference etc. Eavesdropping attacks can also be defined as interception and reading of messages and conversations by unintended receivers [2]. This information can include the node's private key, public key, location, or password. By clicking the communication line, the classified data can be tapped, and it is easier to click the wireless link.

Table 2:Attacker attack on communication between Source and destination another type of attack is called Jamming this attack is a class of DoS attacks that are introduced by malicious node. this attack, jammer broadcasts signals along with security threats [3].Active interference is a DoS attack which distorting and blocks the wireless communication channel.

(ii) Data Link Layer Attack: -

ARP Spoofing: Address Resolution Protocol (ARP) is a protocol that is used to map an IP address to a MAC machine address recognizable in the local Ethernet. When a host machine needs to find a physical Media Access Control (MAC) address for an IP address, it broadcasts an address resolution protocol request [4]. The other host that owns the IP address sends an ARP reply message with its physical address. Every host node on network maintains a table, called 'ARP cache'. The table holds the IP address and associated MAC addresses of another node on the network. ARP spoofing attack may be worked in two ways, cheating the gateway, and cheating the host of the internal network [5]. ARP spoofing may allow an attacker to masquerade as legitimate host and then intercept data frames on a network, modify or stop them. Often the attack is used to launch other attacks such as man-in-the-middle, session hijacking, or denial of service [6].

Selfish Misbehavior nodes may reject to the forwarding method or we can say drops the packets deliberately and to preserve the battery power. Attacks of these types are directly affecting the self-performance of nodes and do not interfere with the process of the network. Except for Dynamic Source Routing (DSR), most routing protocols have no mechanism to detect whether a packet is being forwarded.

Malicious Behavior of Nodes The major task of the malicious node is to disturb the normal operation of routing protocol[7]. When communicating between neighboring nodes, the impact of such attacks increases. This type of attack is a denial of service (DoS):These types of threats use the infected nodes to produce malicious behaviors, thus posing a serious security risk.

(iii) Misdirecting Traffic:

A malicious node will broadcast wrong routing information in order to obtain secure data before actual routing. These nodes receive the information that was intended for the owner of the address. A malicious node advertises fake request, so that the other nodes will direct the replies to the nodes.

Another types of network attack on data link layer is DHCP starvation attacks and dynamic host configuration protocol spoofing attacks which is targeted to DHCP servers is known as DHCP starvation attack.

Ina DHCP starvation attack, an attacker broadcasts large number of DHCP REQUEST messages with spoofed source MAC addresses.

(iv) Network layer attack: -

The responsibility of the network layer is to transmit the packets from source node to the destination node with finding the best route. The attacker disrupts the path between source node to destination node that is choose from the routing protocols [14].

Blackhole Greyhole attack: Black hole and Greyhole attacks are network layer attacks, which destroy performance due to dropped packets. The black hole and Grey are considered in wireless networks. The effectiveness of the network will be decreased during blackhole attack, important packets will not reach the destination. Network parameters such as delay and throughput will be changed during the blackhole attack. The delay will be increased because the packets will not be delivered to the destination. The throughput will be become very less, while it will be used from the blackhole attacker. [8] [9]. The difference is that the Greyhole

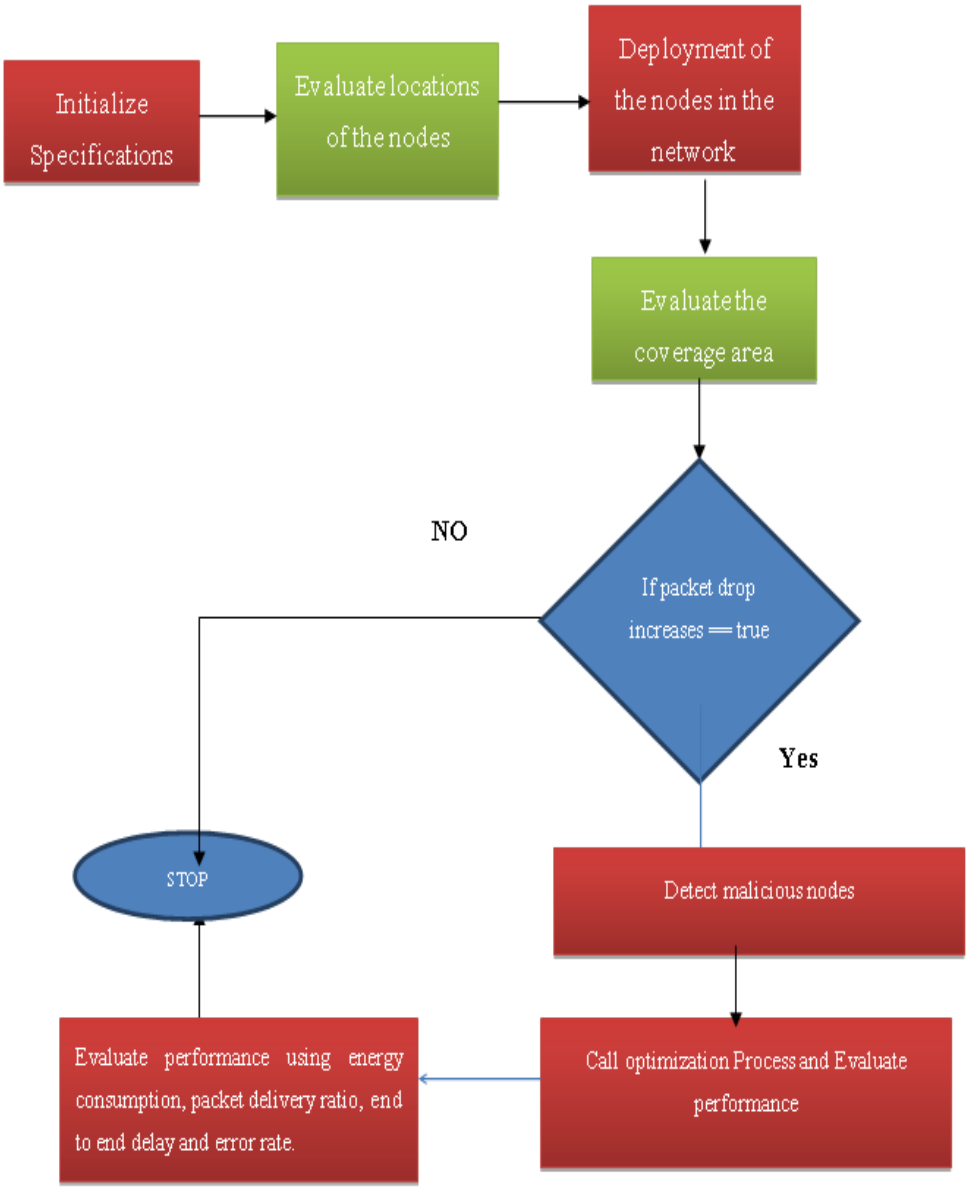
does not drop the entire packet, but drops part of the packet. The packet is dropped by the wrong node, which is called the attacker node. Black hole and Greyhole attacks will have a great impact on the performance of Mesh wireless networks.

(v) Sybil Attack: -

Trust and Sybil attacks are two types of impersonation attack. Sybil Attack is an attack seen in a peer-to-peer network, where nodes in the network actively operate multiple identities at the same time and destroy the authority/powers in the reputation systems. In Sybil attacks, a malicious node claims a large number of client identities, either by impersonating other legal nodes or claiming false identities[10 [11]. The sybil attack attacker creates fake multiple identities of valid nodes. In sybil nodes mislead valid nodes into believing that nodes have many neighbors.

Proposed Work on sybil attack: - This paper deals with one of the harmful security threats known as Sybil attack and proposes an algorithm method to hamper a Sybil attack in a wireless sensor network.

The below is the methodology Flow Diagram of the proposed work.



5. Methodology Diagram

1. Initially we will configure the network using specifications like network length, network width, initial energy of nodes
2. Then we will deploy the nodes in the network
3. Then we will find the nodes having maximum energy than the average energy in the network
4. Then we will implement the coverage area in which each node is having coverage nodes i.e. which node is coming in the coverage of which node and at what distance it is coming

5. Then we will implement the attack scenario in which we will find the malicious nodes
6. Then we will evaluate the network performance in terms of energy consumption, packet deliveries, control overhead
7. In the next step we will perform the hybrid optimization swarm intelligence approach for the optimize routing which make use of the key distribution process in which the mitigation of the attack will take place
8. Then we will compare the performance of the proposed approach in the presence of attack and after optimization.

6. Simulation Environment

Routing in ad-hoc networks is very puzzling due to the characteristic that differentiate these systems from various wireless systems like cellular networks. Because of comparatively large sensor nodes in number, it is very difficult or sometimes not even possible to build a worldwide addressing arrangement for the placement of a large number of nodes in the sensor network as the overhead can be increases and collisions of the packets can be high. So, there must be highly efficient protocols needed for the routing scenarios through which we will get high throughput and less error rate probabilities.

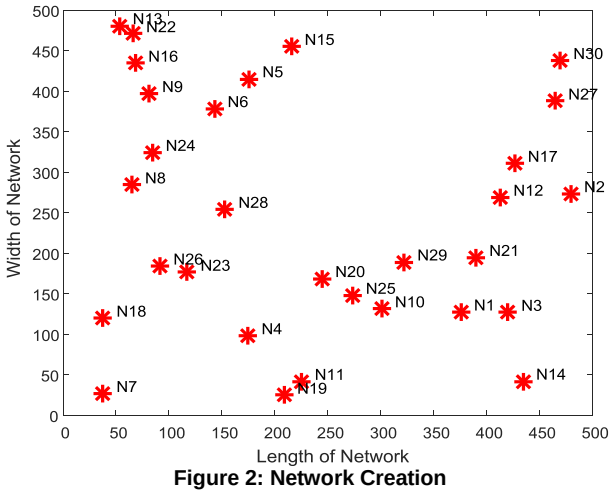


Figure 2: Network Creation

Due to various circumstances, many new procedures have been planned for the routing difficulty in sensor networks. These Routing apparatuses have taken into attention in terms of the inherent topographies of sensor networks along with the submission and construction requirements. The task of maintaining directions in sensor networks is very difficult since energy limitations and sudden variations in node directivities and locations cause frequent attacks and random topological variations.

Figure 2 shows the network creation and deployment of the sensor nodes and shows that the nodes are deployed randomly and the network is heterogeneous in nature because the nodes in the mobile ad-hoc networks are mobile in nature. In figure 2 shows the nodes are deployed which are red in colour and their locations are calculated randomly. The area is taken as 500 meters in length and width of the network. This can vary according to the node's density in the network. So, the routing and deployment of the nodes is one of the main aspects in the mobile ad-hoc networks for the high reliability and proper communication with the base station or sink in efficient manner.

7. Simulation Results

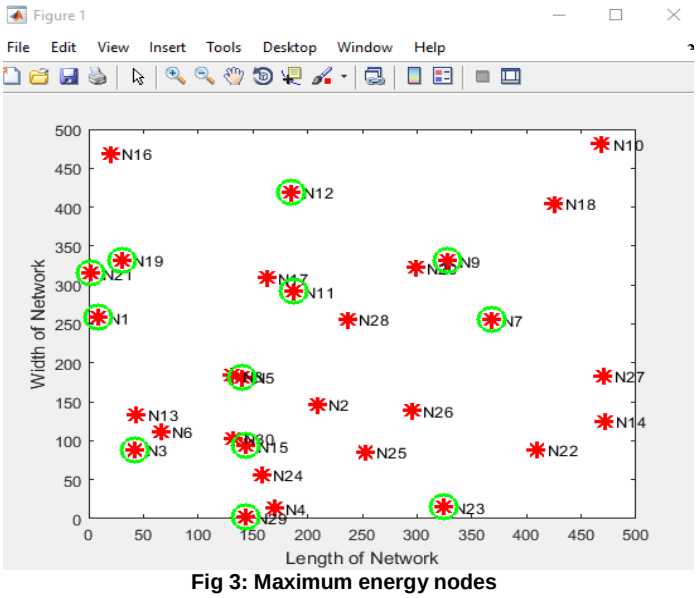


Fig 3: Maximum energy nodes

Fig 3 shows the network nodes in which the nodes which are having maximum energies are marked in the green colour and shows that these nodes are having high capability of achieving high broadcasting of the nodes and the request in the network. This step is one of the crucial steps in which the system is able to achieve high energy conservation.

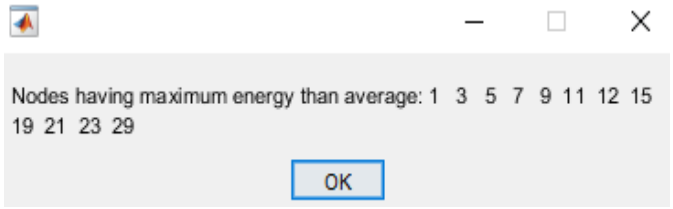


Fig 4: Node Id's

The fig 4 shows the node id's having maximum energy in the network. Through these nodes the routing will be performed and we are able to achieve high energy conservation.

Variables - cov_area_nodes

cov_area_nodes

30x30 double

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
1	0	0	0	5	0	0	0	9	10	0	0	13	0	0	0	0
2	0	0	0	0	0	7	0	9	0	0	0	0	0	0	0	0
3	0	0	4	5	6	0	8	0	10	0	12	0	14	15	16	0
4	0	3	0	5	6	0	8	0	0	0	12	0	14	15	16	17
5	0	3	4	0	6	0	0	0	10	0	12	0	14	15	16	0
6	0	3	4	5	0	0	8	0	0	0	12	0	14	15	16	0
7	2	0	0	0	0	0	0	0	0	11	0	0	0	0	0	0
8	0	3	4	0	6	0	0	0	0	0	12	0	14	15	0	0
9	2	0	0	0	0	0	0	0	10	0	0	13	0	0	0	0
10	0	3	0	5	0	0	0	9	0	0	0	13	0	0	16	0
11	0	0	0	0	0	7	0	0	0	0	0	0	0	0	0	17
12	0	3	4	5	6	0	8	0	0	0	0	0	14	15	16	0
13	0	0	0	0	0	0	0	9	10	0	0	0	0	0	0	0
14	0	3	4	5	6	0	8	0	0	0	12	0	0	15	16	0
15	0	3	4	5	6	0	8	0	0	0	12	0	14	0	16	0
16	0	3	4	5	6	0	0	0	10	0	12	0	14	15	0	0
17	0	0	4	0	0	0	0	0	0	11	0	0	0	0	0	0
18	2	0	0	0	0	7	0	9	0	0	0	0	0	0	0	0

Fig 5 (a) Coverage node id's

dist_mat_nodes

30x30 double

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	1
0	0	0	0	197.2153	0	0	0	187.1062	136.2231	0	0	67.5991	0	0	0	0	
0	0	0	0	0	0	188.4201	0	104.7210	0	0	0	0	0	0	0	0	20
0	0	0	196.6559	71.7262	115.6655	0	199.0218	0	170.8045	0	43.3436	0	123.0288	119.6104	78.1811	0	
0	0	196.6559	0	183.7902	145.4699	0	132.1613	0	0	0	184.3764	0	195.3297	119.8831	173.5625	161.0417	
0	0	71.7262	183.7902	0	160.9258	0	0	0	107.3689	0	107.4048	0	183.9971	153.6306	11.8739	0	
0	0	115.6655	145.4699	160.9258	0	0	86.1423	0	0	0	76.4450	0	49.9255	25.6814	159.0777	0	
0	188.4201	0	0	0	0	0	0	0	0	150.3671	0	0	0	0	0	0	176
0	0	199.0218	132.1613	0	86.1423	0	0	0	0	0	162.1915	0	115.1651	80.2019	0	0	
0	104.7210	0	0	0	0	0	0	0	120.8038	0	0	134.9777	0	0	0	0	92
0	0	170.8045	0	107.3689	0	0	0	120.8038	0	0	0	132.6585	0	0	109.3936	0	
0	0	0	0	0	0	150.3671	0	0	0	0	0	0	0	0	0	106.9315	
0	0	43.3436	184.3764	107.4048	76.4450	0	162.1915	0	0	0	0	0	79.8280	86.2750	110.6652	0	
0	0	0	0	0	0	0	0	134.9777	132.6585	0	0	0	0	0	0	0	
0	0	123.0288	195.3297	183.9971	49.9255	0	115.1651	0	0	0	79.8280	0	0	75.6040	185.1500	0	
0	0	119.6104	119.8831	153.6306	25.6814	0	80.2019	0	0	0	86.2750	0	75.6040	0	149.9791	0	
0	0	78.1811	173.5625	11.8739	159.0777	0	0	0	109.3936	0	110.6652	0	185.1500	149.9791	0	0	
0	0	0	161.0417	0	0	0	0	0	0	106.9315	0	0	0	0	0	0	
0	20.3981	0	0	0	0	176.0252	0	92.1067	0	0	0	0	0	0	0	0	

Fig 5 (b) Distance Coverage

(b) Distance Coverage

The fig 5(a) shows the nodes coverage area in which the matrix is shown in terms of coverage area. In this it can be seen that the nodes which are coming to neighbour nodes are having coverage scenarios. For example, in the first column node id 1 is given and in the front of the row 1 column the node ids are given which is coming in the coverage of the node 1.

Fig 5(b) shows the coverage area nodes in which the instead of ids distances are given and shows that which node is coming in the coverage area of which node and at what distance. The distances are measured in meters.

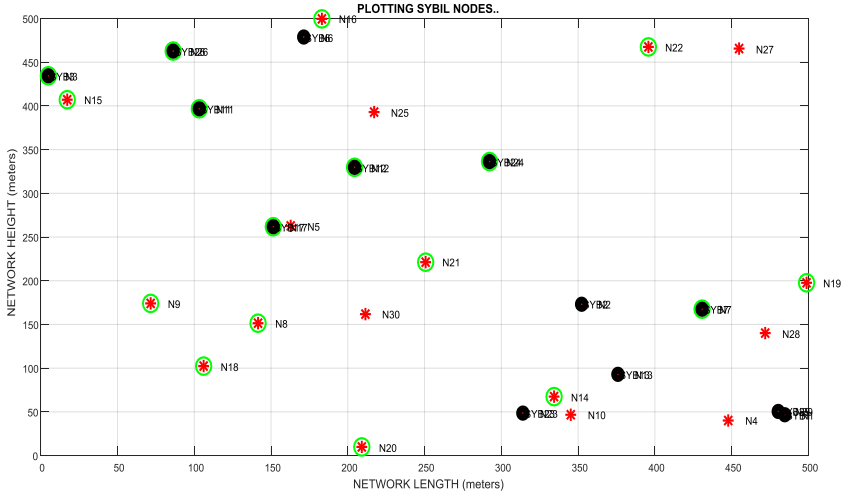


Fig 6: Sybil Attack Nodes

Fig 6 shows the Sybil nodes in the network which shows that the nodes in the black colour are the duplicate ids of the original nodes and are able to perform the attack scenario and perform congestion and routing overhead in the network

In the coming part, we are going to analyse the performance in the sensor network in the presence of attack and then evaluate the performance of the system in terms of the energy consumption, packet delivery rate, and end delay. So, we have achieved second objective and will move the third objective in the coming scenarios.

8. Conclusion

In this Paper we study various MANET applications and their attacks. We deploy network nodes randomly and the network is heterogeneous on the networkthe area is taken as 500 meters in length and width of the network. This can vary according to the node's density in the network. After that we found nodes which are having high capability of achieving high broadcasting, high energy, coverage node id's, distance coverage id's and found sybil attack nodes and the request in the network. Further we will compare with any other algorithm and comparison old and new algorithms.

References

[1] Chen, Yuh-Shyan, and Yun-Wei Lin. "Mobicast routing protocol for mobile ad-hoc networks." IEEE Sensors journal 13, no. 2 (2013): 737-749.

[2] VikrantGokhale, S.K.Gosh, and Arobinda Gupta, "Classification of Attacks on Wireless Mobile Ad HocNetworksandVehicular Ad Hoc Networks aSurvey".

[3] Bhuyan, Monowar H., Dhruba Kumar Bhattacharyya, and Jugal K. Kalita. "Information metrics for low-rate DDoS attack detection: A comparative evaluation." In Contemporary Computing (IC3), 2014 Seventh International Conference on, pp. 80-84. IEEE, 2014.

[4] Climent, Salvador, Antonio Sanchez, Juan Vicente Capella, Nirvana Meratnia, and Juan Jose Serrano. "Underwater acoustic wireless sensor networks: advances and future trends in physical, MAC and routing layers." *Sensors* 14, no. 1 (2014): 795-833.

[5] M. Conti, N. Dragoni and V. Lesyk, "A Survey of Man In The Middle Attacks," in IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 2027-2051, thirdquarter 2016.

[6] Kavar, Jaydip M., and K. H. Wandra. "Survey paper on Underwater Wireless Sensor Network." (2012)

[7] Shikha Sharma, Manish Mahajan, "A Study of Attacks at Different Layers in Mobile Ad-Hoc Network," International Journal of Advanced Research in Computer Science and Software Engineering, vol. 6, Issue 6,June 2016.

[8] Bridges, Susan, Rayford B. Vaughn," Intrusion Detection via Fuzzy Data Mining", In Proceedings of 12th Annual Canadian Information Technology Security Symposium, pp. 109-122, Ottawa, Canada, 2000.

[9] Curiac, Daniel-Ioan. "Wireless sensor network security enhancement using directional antennas: State of the art and research challenges." Sensors 16, no. 4 (2016): 488.

[10]. Rupinder Kaur, Parminder Singh, (2014)" Black Hole and Greyhole Attack in Wireless Mesh Network", American Journal of Engineering Research (AJER), Volume-3, Issue-10, pp-41-47 [11]. RuPurva Sharma (2014)" Survey on Orthogonal Dimensions of Sybil Attack in Wireless Sensor Network", International Journal of Computer Applications, National Conference on Intelligent Systems.

[12] Gorine, Habib, and M. Ramadan Elmezughi. "Security threats on wireless sensor network protocols." World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering 10, no. 8 (2016): 1483-1486.

[13] Cheng, En, Xizhou Lin, Shengli Chen, and Fei Yuan. "A TDoA Localization Scheme for Mobile ad-hoc networks with Use of Multilinear Chirp Signals." Mobile Information Systems 2016 (2016).

[14]. Christiana Ioannou and VasosVassiliou (2016),"The Impact of Network Layer Attacks in Wireless Sensor Networks". 2016 International Workshop on Secure Internet of Things (SIoT), IEEE.

[15] Dong, Wei, and Xiaojin Liu. "Robust and secure time-synchronization against sybil attacks for sensor networks." *IEEE Transactions on Industrial Informatics* 11.6 (2015): 1482-1491.

[16] Patel, S. T., & Mistry, N. H. (2017, February). A review: Sybil attack detection techniques in WSN. " *In Electronics and Communication Systems (ICECS)* 2017 4th International Conference on (pp. 184-188)