Shiv Shakti International Journal of Multidisciplinary and Academic Research
(A Peer Reviewed Journal)
ISSN: 2278-5973 (Online) | Vol. 13, No. 6, (November 2025)

Deep Study and Classifications of Detectin the Techniques of Flooding Attack in Manet

Dr. Gurpreet Singh
Assistant professor , Department of Computer Science ,
DIPS College (Co-edu), Dhilwan, Kapurthala, Punjab.

Abstract

In a MANET number of devices or mobiles are connected to each other with wireless medium. This network is a temporary network. In the MANET, there is not any centralized device which control all netwrok. MANET using dynamic topology. The MANET using the radio transmission range.Here every device takes part in directing by sending information to different device. Every hub in MANET will go about as host just as switch. So it is not much safe Network. The attacker are easily attacks on the MANET. Consequently, Security is an essential worry to give ensured correspondence between nodes in impromptu organizations and shots at having the weaknesses are additionally more.The attackers are used number of attacks on the MANET which destroyed the network. In this paper we analysis and complete study of the various attacks and decline the network performance and throughput.

INTRODUCTION

MANET (Mobile Ad hoc Networks) is the wireless networks. It has not any centralized and fixed network. The mobile devices in a MANET self arrange together in some self-assertive design. A MANET is a self-sufficient assortment of mobile clients that convey over generally data transmission obliged remote connections. Since the devices are mobile, the MANETtopology may switch quickly and unusually over the long haul. These MANETs can be applied between people or between vehicles in regions which are drained of fixed framework. Two devices can straightforwardly speak with one another on the off chance that they are inside the radio span. In the event that the devices are not inside the radio span they can speak with one another utilizing multi hop routing. The remote connection between the devices in Mobile adhoc networks profoundly vulnerable.. This is on the grounds that device can consistently move causing the successive breakage of the connection. The force accessible for transmission is likewise stringently restricted. The topology of the organization is exceptionally unique because of the constant breakage and foundation of remote connection Nodes persistently move into and out of the radio span. This leads to the change in routing data. The MANET is decentralized; where all organization movement including finding the topology and conveying messages should be executed by the actual device for example steering usefulness will be fused into mobile device. MANET is more powerless than wired organization because of versatile device, dangers from vindictive device inside the organization. Due to weaknesses, MANET is more inclined to vindictive assaults. MANET has following weaknesses [1]

- Limited Resources
- Dynamic topology
- Fixed Bandwidth
- No fixed Boundary
- Lack of centralized node
- Limited power supply
- Attackers in the networks

Corresponding Author: Dr. Gurpreet Singh, *see_gurpreet@yahoo.com*

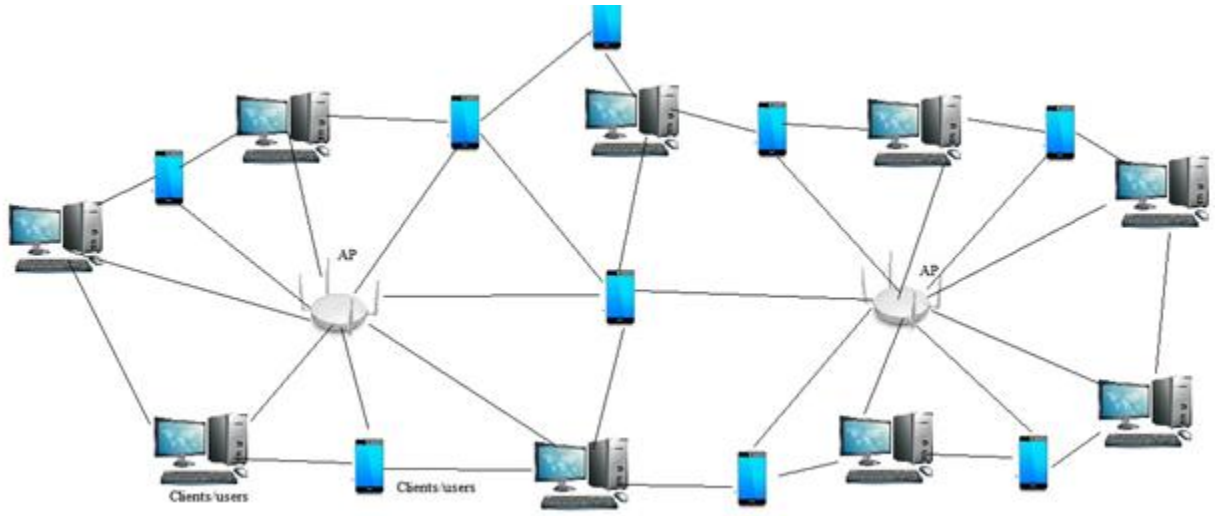
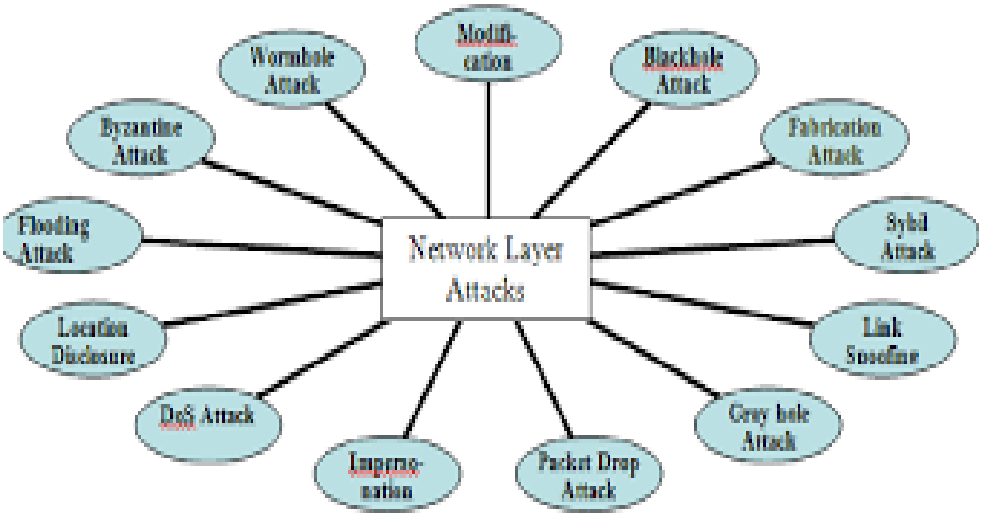


Figure : MANET

There are various attacks who disturb the MANET because in MANET using dynamic topologies, there is no central computer system to handle, no perfect algorithm to mange the network. The various attacks are disturb the different layers. The following attacks in MANET.

MANET attacks



MANET regularly suffers from security attacks because of its characteristics like exposed medium, dynamic topology, absence of the central managing system, non-cooperative algorithms, and absence of strong protection mechanism. Numerous attacks on the different MANET layers are presented in figure[2]

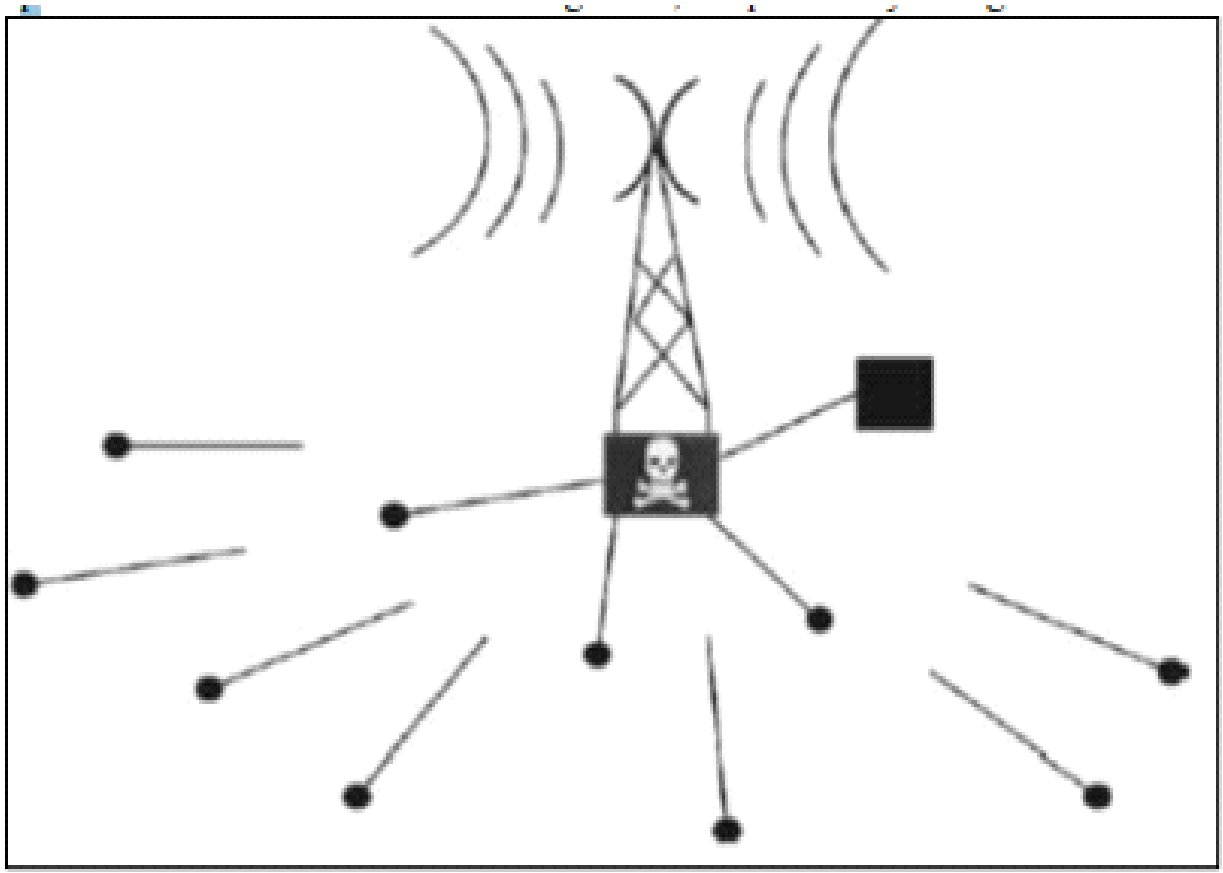
ATTACKES IN VARIOUS LAYES IN MANET

The following layer wise attacks that are responsible for the low performance in MANET. These attacks are worked in the different layers like-

Layer Wise Attacks		
1.	Physical Link Layer	1. Jamming 2. Eavesdropping 3. Tampering
2.	Data Link Layer	1. Denial of Service 2. Misrouting Traffic 3. Misbehavior 4. Selfish node Behavior
3.	Network Link Layer	1. Black Hole 2. Sybil 3. Wormhole 4. Grey hole **5. Flood** 6. Sinkhole
4.	Transport Link Layer	1. Session Hijacking 2. Flooding
5.	Application Link Layer	1. Virus 2. Data Corruption 3. Malicious Behavior 4. Cloning

Flood Attack

In Flooding attack implies one device is sending messages todifferent devices. That node is not a valid node or legal in the Mobile Adhoc Network. This illegal node is sending the packets to any legal node and breaks the security of MANET. It simply re-broadcast overhead packets with enough power to be received by every other node in the network.This Flooding attack uses packets as a weapon to convince MANET. In Flooding attack an attacker use a high radio transmission range and processing power sends packets to a lot of Mobile Adhoc Network nodes which are dispersed in a large area within a Mobile Adhoc Network.The flooding attack can easily be launched by an attacker node, but this attack causes the most damage to the MANET. This attack can be implemented by using the excess of RREQs (Route Requests) or data flooding. In RREQ flooding attack, the malicious node floods the RREQs in the network, which results in consuming a lot of network resources. This attack is launched by selecting IP addresses which do not exist in the MANET and due to this, no node is able to reply RREP (Route Reply) packets against these flooded RREQs. In data flooding attack, the malicious node establishes various paths with the number of nodes in the network. Once paths get established, the malicious node starts transferring a large number of useless data packets in order to reduce the performance of the network. These large numbers of data packets make congestion in the network. The main aim of this attack is to degrade the performance of the network by exhausting various network resources.



Literature Review

Abdulai, Ould-Khaoua & Mackenzie (2009) suggested new probabilistic techniques that employ on flooding method. In the proposed method, a mobile node takes the responsibility of broadcasting received RREQ packets. The broadcasting process continues until it discovers a route to exact destination. Continuous broadcasting leads to contention of high channel, duplicate retransmissions, thus causing too much packet collisions in the manet. The proposed method equipped AODV with a appropriate probabilistic route detection method which showed significant performance improvement by achieving good throughput and reduced routing overhead. The MAC collisions and minimal end-to-end delay.

Jiang, Lin & Wu (2014) demonstrated that MANETs are vulnerable to threats from flooding attack done by compromised nodes since the network is organized without any centralized coordinator. If the source node wants to transmit data, RREQ is disseminated to all of its neighbors. If the flooding attack is launched by the intruder node enters with out-of-domain IP address as its destination address, then it tries to flood huge number of packets into the network. The intermediate nodes perform forwarding process lead to consumption of energy and processing resources. In the proposed technique, redundant RREQ packets are suppressed depending on the cooperation of destination and neighbour nodes within one hop distance of the intruder node. A petri net design has been incorporated to model the proposed technique and registers the entire processing aspects of a system for a quantitative and more concise analysis. The relevant simulations were conducted for quantitative analysis using NS-2 simulator. The planned power-saving method has experimentally verified to expand the lifetime of MANET in flooding attack.

Giuseppe Bianchi (2000):- The essential medium access control (MAC) strategy of 802.11 is called dispersed coordination work (DCF). DCF is a transporter sense various access with crash aversion (CSMA/CA) conspire with parallel opened outstanding back off. This paper gives a straightforward, hootwaver all things considered very precise, scientific model to figure the 802.11 DCF throughputs, in the suspicion of limited number of terminals and ideal channel conditions. The proposed examination applies to both the bundle transmission plans utilized by DCF, in particular, the essential access and the RTS/CTS access instruments. IEEE has normalized the 802.11 convention for Wireless Local Area Networks. What's more, it additionally applies to a blend of the two plans, wherein bundles longer than a given limit are communicated by the RTS/CTS component.

Deepak Bansal and Hari Balakrishnan (2000) :- Binomial calculations sum up TCP-style added substance increment by expanding conversely corresponding to a force k of the current window (for TCP, k = 0); they sum up TCP-style multiplicative-decline by diminishing relative to a force l of the current window (for TCP, l = 1). It was show that there are an endless number of deployable TCP-accommodating binomial calculations, all of which fulfill k + l = 1, and that all binomial calculations meet to reasonableness under a synchronized-criticism supposition gave k + l > 0; k; l 0. Our recreation results show that binomial calculations communicate it was with TCP across a RED passage. It was center around two specific calculations. Analyses of a class of nonlinear clog control calculations called binomial calculations, propelled to a limited extent by the requirements of it wasbased sound and video applications for which a radical decrease in transmission rate upon blockage is risky. IIAD (opposite increment/added substance decline, k = 1; l = 0) and SQRT (k = l = 0:5), showing that they are appropriate to applications that don't respond it was to huge TCP-style window decreases. It was likewise find that TCP-invitingness as far as the connection among throughput and misfortune pace of a calculation doesn't really suggest reasonableness comparative with TCP execution, particularly for drop-tail bottleneck doors S. Floyd (1994):- The distributed limit structure for giving various degrees of best-exertion administration in the midst of organization clog. The "dispensed limit" structure—augmentations to the Internet conventions and calculations can assign data transfer capacity to various clients in a controlled and unsurprising manner during network clog. The structure upholds two corresponding methods of controlling the data transfer capacity distribution: sender-based and collector based. In the present heterogeneous and business Internet the structure can fill in as a reason for charging for use and for all the more productively using the organization assets. It was center around calculations for fundamental segments of the system: a differential dropping calculation for network switches and a labeling calculation for profile meters at the edge of the organization for mass information moves. It was present reproduction results to represent the adequacy of the joined calculations in controlling transmission control convention (TCP) traffic.

C. E. Perkins and E. M. Royer, (1999) :-It was present Ad-hoc On Demand Distance Vector Routing (AODV), a novel calculation for the activity of such Ad Hock organizations. Every portable host works as a specific switch, and courses are acquired depending on the situation (i.e., on-request) with next to zero dependence on intermittent ads. Our new directing calculation is very appropriate for a unique self-beginning organization, as needed by clients wishing to use specially appointed organizations. AODV gives circle free courses even while fixing broken connections. Since the convention doesn't need worldwide occasional steering ads, the interest on the general transmission capacity accessible to the versatile hubs is considerably not exactly in those conventions that do require such commercials. In any case it was can in any case keep up a large portion of the upsides of fundamental distance vector steering instruments. Ad Hock on Demand Distance Vector Routing, Proc. IEEE Workshop on Mobile Computing Systems and Applications, An Ad Hock organization is the agreeable commitment of an assortment of portable hubs without the necessary intercession of any concentrated passage or existing framework.It was show that our calculation scales to

huge populaces of versatile hubs wishing to frame Ad Hock organizations. It was likewise incorporate an assessment procedure and reenactment results to confirm the activity of our calculation.

Andras Veres (2001):- This paper explores separated administrations in remote parcel networks utilizing a completely dispersed methodology that backings administration separation, radio checking, and affirmation control. While our proposition is by and large relevant to circulated remote access plans, it was configuration, execute, and assess our system inside the setting of existing remote innovation.

Administration separation depends on the IEEE 802.11 appropriated coordination work (DCF) initially intended to help best-exertion information administrations. It was break down the postponement experienced by a portable host executing the IEEE 802.11 DCF and infer a shut structure equation. It was at that point stretch out the DCF to offer support separation for delay-delicate and best-exertion traffic dependent on the outcomes from the examination. Two conveyed assessment calculations are proposed.

These calculations are assessed utilizing recreation, investigation, and experimentation. A virtual MAC (VMAC) calculation latently screens the radio channel and gauges locally reachable help levels. The VMAC gauges key MAC level measurements identified with administration quality like deferral, postpone variety, parcel impact, and bundle misfortune. It was show the proficiency of the VMAC calculation through recreation and consider essentially covering cells and profoundly burst traffic blends. Likewise, it was carry out and assess the VMAC in a trial separated administrations remote proving ground. A virtual source (VS) calculation uses the VMAC to appraise application-level assistance quality. The VS permits application boundaries to be tuned because of dynamic channel conditions dependent on "virtual defer bends." It was show through reenactment that when these circulated victual calculations are applied to the confirmation control of the radio channel then a worldwide stable state can be kept up without the requirement for complex brought together radio asset the board.

Oretis Tsigkas (2006):- Most existing access systems can't give Quality-of-Service (QoS) affirmations. Indeed, even those that are QoS mindful can just offer relative assistance separation. In this work, it was propose a point wasfull need medium access plan to give time-limited administrations. By approximating an ideal Earliest Deadline First (EDF) scheduler, the proposed plan can offer deferral and postpone jitter affirmations while accomplishing high medium usage. Scientific investigations and reproduction tests report and affirm the positive attributes of the proposed instrument. Wireless Local Area Networks have acquired fame at an uncommon rate in the course of the most recent couple of years. Nonetheless, as the range of utilizations they are called to help widens, their failure in gathering the assorted necessities of a more extensive scope of uses gets obvious.

Gangh Seop Ahn (2002):- This paper is describes SWAN upholds per-jump and start to finish control calculations that essentially depend on the proficient activity of TCP/IP conventions. Specifically, SWAN utilizes neighborhood rate control for best-exertion traffic, and sender-based confirmation control for constant UDP traffic. Express clog warning (ECN) is utilized to progressively control conceded ongoing meetings despite network elements it welcomed on by portability or traffic over-burden conditions. SWAN doesn't need the help of a QOS-skilled MAC to convey administration separation. Maybe, constant administrations are constructed utilizing existing best exertion remote MAC innovation.SWAN, a stateless organization model which uses disseminated control calculations to convey administration separation in portable remote specially appointed organizations in a basic, adaptable and hearty way. The proposed engineering is intended to deal with both constant UDP traffic, and best exertion UDP and TCP traffic without the requirement for the presentation and the executives of per-stream state data in the organization Reenactment, examination, and

results from a trial remote proving ground show that ongoing applications experience low and stable deferrals under different multihop, traffic, and versatility circumstances.

Mohseni, et al., (2010):- Focused on routing, a challenging effort that seen several schemes claiming to offer development over others. Competing schemes create tough to decide for the best performs within multiple network conditions as described by QoS contributions. Furthermore, a performance comparison on routing protocol schemes was offered and recommendations it was performed to attain protocols performance improvement.

Charles Adward and Eliizabeth M (1999):- A specially appointed organization is the helpful commitment of an assortment of versatile hubs without the necessary mediation of any incorporated passage or existing framework. It was present Ad-hoc On Demand Distance Vector Routing (AODV), a novel calculation for the activity of such impromptu organizations. Every portable host works as a particular switch, and courses are acquired on a case by case basis (i.e., on-request) with almost no dependence on intermittent ads. Our new directing calculation is very appropriate for a unique self-beginning organization, as needed by clients wishing to use specially appointed organizations. AODV gives circle free courses even while fixing broken connections. Since the convention doesn't need worldwide occasional directing ads, the interest on the general transmission capacity accessible to the portable hubs is considerably not exactly in those conventions that do require such notices. All things considered it was can in any case keep up the majority of the benefits of essential distance vector directing instruments. It was show that our calculation scales to huge populaces of versatile hubs wishing to shape specially appointed organizations. It was likewise incorporate an assessment system and reenactment results to confirm the activity of our calculation.

Frank P. Kelly, Peter B. Key and Stan Zachary (2000):- Structure for confirmation control for a bundle based organization where the choices are taken by edge gadgets or end-frameworks, as opposed to re-sources inside the organization. The choices depend on the aftereffects of test parcels that the end-frameworks send through the organization, and require just that assets apply an imprint to bundles in a manner that is load subordinate. One application model is the Internet, where stamping data is taken care of back through an ECN spot, and it was show how this methodology permits a rich QoS system for ows or streams. Our methodology permits organizations to be expressly examined, and thus designed.

C.R. Lin and M. Gerla (1995):- Self-arranging, multihop, portable radio organization which depends on a code-division access conspire for interactive media support. In the proposed network design, hubs are coordinated into no covering bunches. The bunches are autonomously controlled, and are progressively reconfigured as the hubs move. This organization engineering enjoys three fundamental benefits. To begin with, it gives spatial reuse of the data transmission because of hub grouping. Second, data transmission can be shared or saved in a controlled style in each bunch. At long last, the bunch calculation is hearty even with topological changes brought about by hub movement, hub disappointment, and hub addition/evacuation. Recreation shows that this engineering gives a proficient, stable framework for the joining of various sorts of traffic in a unique radio organization.

Shrivastava, et al., (2011):- Introduced MANET enactment for routing protocols disgraced with improving stream of traffic it weight. Itwas-knownit wasAODV, DSDV, and DSR and their performance comparison it was carried out for changing traffic loads. Simulations it was made using a NS-2 simulator. Reactive protocols had outperformed it was over proactive protocols.

Gandhewar & Patel, (2012):- Discussed on sinkhole issue, its results and scheme for AODV protocol context recognition/anticipation. It revealedAODV performance without sinkhole attack, in attack and after mechanism application via simulation for particular network node variant by taking performancemeasures such as PDR,for End delay and Packet loss. The simulation had been completed with NS2 simulator.

Dhenakaran & Parvathavarthini, (2013):- Focused on routing methods, the most challenging problem because of ad hoc networks dynamic topology. Several schemes it was provided for effective routing claiming enhanced performance and also various MANETs routing protocols made it tough to fix on suitable multiple network enter ions. The methods had provided a review of several routing protocols in survey and offered a comparison among them.

Han& Lee (2013) presented an adaptive Hello messaging system to hold back the redundant Hello messages without decreased broken links detect capability. The experiments revealed that the novel system minimized energy utilization and network overhead without any throughput divergence.

CONCLUSION

The MANET is an open and portability network, the MANETs are significantly more liable to all sort of safety hazards, like data leakage, interruption, or even DoS attacks.. As a result, the security needs in the mobile ad hoc networks are much higher than those in the traditional wired networks. Due to continue growth of mobile adhoc networks, the need for more effective security mechanisms is also increasing. In this paper we have examined the different types of techniques of flooding attacks in MANETs. A detail study of countermeasures for this attack is required in order to minimize or eliminate their impact. More efficient and robust techniques for the countermeasures of various types of flooding attacks should be proposed in order to make MANETs more secure and their extension in other fields.

References

Jatinder Singh, LakhwinderKaur, and Savita Gupta, "A Cross-Layer Based Intrusion Detection Technique for Wireless Networks", “International Arab Journal of Information Technology”, Volume 9, No. 3, May 2012 and ISSN: 1683-3198.

Gagandeep, Aashima, Pawan Kumar, “Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review”, International Journal of Engineering and Advanced Technology (IJEAT), , Volume-1, Issue-5, June 2012 and ISSN: 2249 – 8958.

KaminiMaheshwar, Divakar Singh, "Black Hole Effect Analysis and Prevention through IDS in MANET Environment", "European Journal of Applied Engineering and Scientific Research", 2012, ISSN: 2278 – 0041.

Satria Mandala, Md. AsriNgadi, A.Hanan Abdullah, “A Survey on MANET Intrusion Detection”, “International Journal of Computer Science and Security”, Volume 2, Issue 1, 2013 and ISSN:1985-1553.

Antony Devassy, K. Jayanthi," Prevention of Black Hole Attack in Mobile Ad-hoc Networks using MN-ID Broadcasting", "International Journal of Modern Engineering Research (IJMER)", Volume 2, Issue.3, May-June 2012, ISSN: 2249-6645.

P. K. Singh and G. Sharma (2012), "An Efficient Prevention of Black Hole Problem in AODV Routing Protocol in MANET", "IEEE International Conference on Trust, Security and Privacy in Computing and Communications".

SachinLalar, “International Journal of Multidisciplinary and Current Research”, “Security in MANET: Vulnerabilities, Attacks & Solutions”, 2014, Vol.2, ISSN: 2321-3124.

PriyankaGoyal, SahilBatra, Ajit Singh, ”A Literature Review of Security Attack in Mobile Ad-hocNetworks”, “*International Journal of Computer Applications”, Volume 9– No.12, November 2010, ISSN:0975-8887.*

Shekharsaini, Rajesh Kumar, “Comparison of layerwise attacks in MANETs”, “ACEEE”, proc. of “*Int. Conf. on Emerging Trends in Engineering and Technology”*

Saritha Reddy Venna, Ramesh BabuInampudi, “A Survey on Security Attacks in Mobile Ad HocNetworks”,”International Journal of Computer Science and Information Technologies (IJCSIT)”, Vol. 7, 2016, ISSN: 0975-9646.

Y. Hu, A. Perrig, D. Johnson (March 2003),*Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks*. Proceedings of The 22nd Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003).

B. Kannhavong, H. Nakayama, Y. Nemoto, N. Kato, A.Jamalipour. A survey of routing attacks in mobile ad hoc networks. Security in wireless mobile ad hoc and sensornetworks, October 2007.

Athira V Panicker, Jisha G, ”Network Layer Attacks and Protection in MANET : A Survey”, “International Journal of Computer Science and Information Technologies”, Vol. 5, 2014, ISSN : 3437-3443.

CH.V. Raghavendran, G. Naga Satish, P. Suresh Varma, “Security Challenges and Attacks inMobile Ad Hoc Networks” **“***I.J. Information Engineering and Electronic Business”*, vol. 3, 2013.

Abhay Kumar Rai, Rajiv RanjanTewari&Saurabh Kant Upadhyay, *Different Types of Attacks on Integrated MANET- Internet Communication ,* International Journal of Computer Science and Security (IJCSS) Volume (4): Issue

G S Mamatha, Dr s c Sharma “Network Layer Attacks And Defense Mechanisms In MANETS-A Survery” International Journal of Computer Applications (0975 – 8887)Volume 9– No.9, November 2010.

SandipNemade, Manish Kumar Gurjar, ZareenaJamaluddin, Nishanth **,**"Early Detection of Syn Flooding Attack by Adaptive Thresholding (EDSAT): A Novel method for detecting Syn Flooding based DOS Attack in Mobile Ad Hoc Network", "International Journal of Advanced Research in Engineering and Technology (IJARET)", Volume 5, Issue 2, February (2014), ISSN 0976 – 6480(Print), ISSN 0976 – 6499(Online).

Neetu Singh Chouhan, ShwetaYadav," Flooding Attacks Prevention in MANET"," International Journal of Computer Technology and Electronics Engineering (IJCTEE)", Volume 1, Issue 3, December 2011, ISSN 2249-6343.

Ming-Yang Su, "Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems", "Elsevier Journal of Computer Communications", Volume 34, Issue 1, January 2011.