Volume 2, Issue 4 April 2016 ISSN NO: 2454 - 7514

North Asian International Research Journal Consortium

North Asian International Research Journal Of Science, Engineering and Information Technology

Chief Editor
Dr. Bilal Ahmad Malik

Publisher

Dr. Bilal Ahmad Malik

Associate Editor

Dr.Nagendra Mani Trapathi

Honorary
Dr.Ashak Hussain Malik

NAIRJC JOURNAL PUBLICATION

North Asian
International
Research Journal Consortium

Nairjc....
North Asian
International
Research
Journal
Consortium

Welcome to NAIRJC

ISSN NO: 2454 -7514

North Asian International Research Journal of Science, Engineering & Information Technology is a research journal, published monthly in English, Hindi, Urdu all research papers submitted to the journal will be double-blind peer reviewed referred by members of the editorial board. Readers will include investigator in Universities, Research Institutes Government and Industry with research interest in the general subjects

Editorial Board

M.C.P. Singh Head Information Technology Dr C.V. Rama University	S.P. Singh Department of Botany B.H.U. Varanasi.	A. K. M. Abdul Hakim Dept. of Materials and Metallurgical Engineering, BUET, Dhaka
Abdullah Khan Department of Chemical Engineering & Technology University of the Punjab	Vinay Kumar Department of Physics Shri Mata Vaishno Devi University Jammu	Rajpal Choudhary Dept. Govt. Engg. College Bikaner Rajasthan
Zia ur Rehman Department of Pharmacy PCTE Institute of Pharmacy Ludhiana, Punjab	Rani Devi Department of Physics University of Jammu	Moinuddin Khan Dept. of Botany SinghaniyaUniversity Rajasthan.
Manish Mishra Dept. of Engg, United College Ald.UPTU Lucknow	Ishfaq Hussain Dept. of Computer Science IUST, Kashmir	Ravi Kumar Pandey Director, H.I.M.T, Allahabad
Tihar Pandit Dept. of Environmental Science, University of Kashmir.	Abd El-Aleem Saad Soliman Desoky Dept of Plant Protection, Faculty of Agriculture, Sohag University, Egypt	M.N. Singh Director School of Science UPRTOU Allahabad
Mushtaq Ahmad Dept.of Mathematics Central University of Kashmir	Nisar Hussain Dept. of Medicine A.I. Medical College (U.P) Kanpur University	M.Abdur Razzak Dept. of Electrical & Electronic Engg. I.U Bangladesh

Address: - Dr. Ashak Hussain Malik House No. 221 Gangoo, Pulwama, Jammu and Kashmir, India - 192301, Cell: 09086405302, 09906662570, Ph. No: 01933-212815,
Email: nairjc5@gmail.com, nairjc@nairjc.com, info@nairjc.com Website: www.nairjc.com

IRJIF IMPACT FACTOR: 3.01

MANET, ITS CHALLENGES, TYPES AND APPROACHES: A SURVEY

***INDERPREET KAUR**
*Research Scholar, PCET, Lalru, Punjab.

****ER.MANASVI MANNAN**
**Astt. Professor, PCET, Lalru, Punjab.

Abstract- ***MANETs are a sort of Wireless specially appointed system that typically has a routable systems administration environment on top of a Link Layer impromptu system. MANETs comprise of a distributed, molding toward oneself, repairing toward oneself system rather than a cross section system has a focal controller (to focus, upgrade, and convey the steering table). MANETs around 2000-2015 ordinarily impart at radio frequencies (30 MHz - 5 GHz).in this paper various review on MANET attacks and protect MANET techniques.***

Index Terms- ***MANET, malicious nodes, PDER, PMOR, PMISR, SVM.***

I. INTRODUCTION

1.1 MANET

A Mobile Ad-hoc Network (MANET) is a set of remote versatile hubs shaping an element self-sufficient system. Hubs speak with one another without the mediation of concentrated access focuses or base stations. Because of the restricted transmission scope of remote system interfaces, numerous bounces are expected to trade information between hubs in the system. Portable Ad hoc Network is the quick becoming innovation from the previous 20 years. The addition in their notoriety is a result of the simplicity of arrangement, foundation less and their element nature.

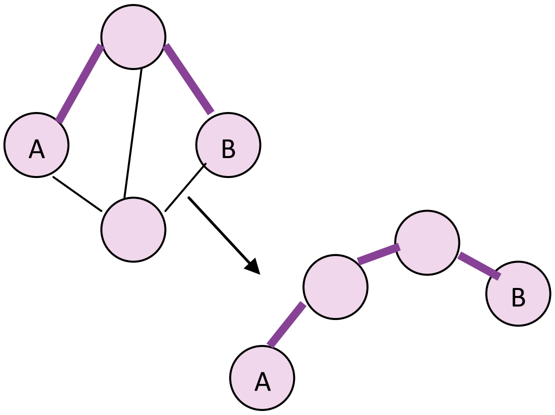

Figure 1.1: MANET

MANET's made another set of requests to be actualized and to give effective better end to end correspondence. The Dynamic Source Routing (DSR) Protocol is a source routed on-interest directing convention. A hub keeps up course reserves containing the source courses that it is mindful of. The node overhauls entrances in the course reserve when it researches new courses. In its bundle head, every given directing parcel has a complete and requested hub list which the bundle will pass definitely.

1.2 Types of MANET

There are different types of MANETs including:

- In VANETs – Intelligent vehicular ad hoc networks make use of artificial intelligence to tackle unexpected situations like vehicle collision and accidents.
- Vehicular ad hoc networks (VANETs) – Enables effective communication with another vehicle or helps to communicate with roadside equipments.
- Internet Based Mobile Ad hoc Networks (I MANET) – helps to link fixed as well as mobile nodes.

1.3 MANET CHALLENGES

- The wireless link characteristics are time-varying in nature: There are transmission impediments like fading, path loss, blockage and interference that adds to the susceptible behavior of wireless channels. The reliability of wireless transmission is resisted by different factors.
- Limited range of wireless transmission – The limited radio band results in reduced data rates compared to the wireless networks. Hence optimal usage of bandwidth is necessary by keeping low overhead as possible.
- Packet losses due to errors in transmission – MANETs experience higher packet loss due to factors such as hidden terminals that results in collisions, wireless channel issues interference, and frequent breakage in paths caused by mobility of nodes, increased collisions due to the presence of hidden terminals and uni-directional links.
- Route changes due to mobility- The dynamic nature of network topology results in frequent path breaks. Frequent network partitions- The random movement of nodes often leads to partition of the network. This mostly affects the intermediate nodes.

1.4 SECURITY GOALS

- **Availability:** Accessibility implies the benefits are open to approved gatherings at fitting times. Accessibility applies both to information and to administrations. It guarantees the survivability of system administration regardless of refusal of administration assault.
- **Confidentiality**: It guarantees that computer related resources are gotten to just by approved gatherings. That is, just the individuals who thought to have admittance to something will really get that get to. To keep up secrecy of some private data, we have to keep them mystery from all elements that do not have benefit to get to them. Secrecy is frequently called mystery or protection [6].
- **Integrity:** Trustworthiness implies that benefits can be altered just by approved gatherings or just in approved way. Change incorporates composing, evolving status, erasing and making.

Trustworthiness guarantees that a message being exchanged is never defiled.

- **Authentication**: Confirmation empowers a hub to guarantee the personality of associate hub it is corresponding with. Validation is basically certification that members in correspondence are confirmed and not impersonators. Validness is guaranteed in light of the fact that just the true blue sender can create a message that will unscramble legitimately with the shared key.
- **Authorization**: This property relegates diverse access rights to diverse sorts of clients. For instance a system administration can be performed by system overseer just.

1.5 Attacks in MANET

- **Passive attack**: in this type of attack, the intruder only performs some kind of monitoring on certain connections to get information about the traffic without injecting any fake information. This type of attack serves the attacker to gain information and makes the footprint of the invaded network in order to apply the attack successfully. The types of passive attacks are eavesdropping, traffic analysis and snooping:
- **Denial of service attack:** Denial of service attacks are aimed at complete disruption of routing information and therefore the whole operation of ad-hoc network.
- **Traffic Analysis:** In MANETs the data packets as well as traffic pattern both are important for adversaries. For example, confidential information about network topology can be derived by analyzing traffic patterns. Traffic analysis can also be conducted as active attack by destroying nodes, which stimulates self-organization in the network, and valuable data about the topology can be gathered. Traffic analysis in ad hoc networks may reveal following type of information.
- **Snooping:** It is similar to eavesdropping but is not necessarily limited to gaining access to data during its transmission. Snooping can include casual observance of an e-mail that appears on another's computer screen or watching what someone else is typing. More sophisticated snooping uses software programs to remotely monitor activity on a computer or network device.
- **Active attack:** in this type of attack, the intruder performs an effective violation on either the network resources or the data transmitted; this is done by International Journal on New Computer Architectures and Their Applications causing routing disruption, network resource depletion, and node breaking. In the following are the types of active attacks over MANET and how the attacker’s threat can be performed
- **Flooding attack:** In flooding attack, attacker exhausts the network resources, such as

bandwidth and to consume a node's resources, such as computational and battery power or to disrupt the routing operation to cause severe degradation in network performance. For example, in AODV protocol, a malicious node can send a large number of RREQs in a short period to a destination node that does not exist in the network. Because no one will reply to the RREQs, these RREQs will flood the whole network. As a result, all of the node battery power, as well as network bandwidth will be consumed and could lead to denial-of-service.

- **Black hole Attack:** Route discovery process in AODV is vulnerable to the black hole attack. The mechanism, that is, any intermediate node may respond to the RREQ message if it has a fresh enough routes, devised to reduce routing delay, is used by the malicious node to compromise the system. In this attack, when a malicious node listens to a route request packet in the network, it responds with the claim of having the shortest and the freshest route to the destination node even if no such route exists. As a result, the malicious node easily misroute network traffic to it and then drop the packets transitory to it.
- **Active attack:** in this type of attack, the intruder performs an effective violation on either the network resources or the data transmitted; this is done by International Journal on New Computer Architectures and Their Applications causing routing disruption, network resource depletion, and node breaking. In the following are the types of active attacks over MANET and how the attacker's threat can be performed
- **Flooding attack:** In flooding attack, attacker exhausts the network resources, such as bandwidth and to consume a node's resources, such as computational and battery power or to disrupt the routing operation to cause severe degradation in network performance. For example, in AODV protocol, a malicious node can send a large number of RREQs in a short period to a destination node that does not exist in the network. Because no one will reply to the RREQs, these RREQs will flood the whole network. As a result, all of the node battery power, as well as network bandwidth will be consumed and could lead to denial-of-service.

- **Black hole Attack:** Route discovery process in AODV is vulnerable to the black hole attack. The mechanism, that is, any intermediate node may respond to the RREQ message if it has a fresh enough routes, devised to reduce routing delay, is used by the malicious node to compromise the system. In this attack, when a malicious node listens to a route request packet in the network, it responds with the claim of having the shortest and the freshest route to the destination node even if no such route exists. As a result, the malicious node easily misroute network traffic to it and then drop the packets transitory to it.

- **Jamming:** Jamming is a special class of DoS attacks which are initiated by malicious node after determining the frequency of communication. In this type of attack, the jammer transmits signals along with security threats. Jamming attacks also prevents the reception of legitimate packets.
- **Malicious code attacks**: malicious code attacks include, Viruses, Worms, Spywares, and Trojan horses, can attack both operating system and user application. Malicious hackers (crackers) frequently use snooping techniques to monitor key strokes, capture passwords and login information and to intercept e-mail and other private communications and data transmissions. Corporations sometimes snoop on employees legitimately to monitor their use of business computers and track Internet usage. Governments may snoop on individuals to collect information and prevent crime and terrorism. Although snooping has a negative aspect in general but in computer technology snooping can refer to any program or utility that performs a monitoring function.

II. RESEARCH ELABORATIONS

Priyanka Sharma et al [1] "Enhanced Security Scheme against jamming attack in Mobile Ad hoc Network" Security is the one of the major concerns in Mobile Ad hoc Network (MANET). In this paper we have proposed an enhanced security scheme against jamming attack with AOMDV routing protocol. The jamming attacker delivers huge amount of unauthorized packets in the network and as a result network gets congested. The proposed scheme identifies the jamming attacker and blocks its activities by identifying the infected or unauthorized packets in network. Multipath routing protocol AOMDV is used to improve the network performance but there is a condition that jamming phase occurs naturally and is not achieved by attacker intentionally.

Meenakshi Patel et al [2]"Detection of Malicious Attack in MANETA Behavioral Approach" Topology of MANET is dynamic in nature due tothis characteristic in this network build routing mechanism more convoluted and anxious and consequently nodes are more vulnerable to compromise and are predominantly susceptible to denial of service attack (DoS) assail launched by malicious nodes or intruders. Reactive routing for instance AODV is trendier than table driven routing exploit flooding to find out route. Proposed method uses machine learning to categorize nodes as malicious. This paper introduced new proposed algorithm for detection of attacks in Ad-hoc networks based on SVM behavioral routing protocols to detect MANET attacks. In this technique we have used the PMOR, PDER, and PMISR as metrics to evaluate the QoS of a link and into prediction of attacks.

Ismail, Z. et al [3] “Impacts of Packet Size on AODV Routing Protocol Implementation in Homogeneous and Heterogeneous MANET" Networks are being utilized as a part of different territories and the interest of clients these days has persuaded the development of the Mobile Ad Hoc Network (MANET). MANET has its own particular directing conventions which can bargained with continuous course trade, dynamic topology, and transfer speed imperative and multi-jump steering. Specially appointed On Demand Distance Vector (AODV) is one of the directing conventions in MANET. The point of this examination is to survey the impacts of diverse bundle size with the usage of AODV steering conventions in homogeneous and heterogeneous MANET through the reenactment strategy.

Thorat, S.A. et al [4] "Outline issues in trust based directing for MANET" In MANET hubs help one another in information steering. MANET functions admirably if the partaking hubs coordinate with one another. It is unrealistic to expect that, all hubs taking an interest in an open MANET are helpful and legitimate. These calculations improve the system execution by using reliable hubs in viable way and punishing non-agreeable hubs. This paper looks at trust based and cryptographic methodologies for actualizing security in MANET steering. The paper talks about configuration issues in trust based steering conventions for MANET in points of interest. The paper shows a review on trust based directing conventions for MANET. The paper gives bearings to future research in trust based directing for MANET.

Durai, K.N. et al [5] "Vitality proficient irregular cast DSR convention with intervention gadget in MANET" Mobile Ad hoc systems (MANET) essentially have dynamic topology, as the directing framework's rundown of neighboring hubs and switches changes its area. The framework proposes a Routing convention in MANET which empowers effective utilization of force and transmission capacity in Mobile Ad-hoc systems (MANET). Randomized Overhearing procedures are proposed to decrease power utilization and upgrade viable Routing in MANET. Randomized catching system is utilized with AODV (Ad-Hoc on Demand Distance Vector) and DSR (Dynamic Source Routing) conventions to decrease the force expended amid transmission in a MANET. Least bounce way is acquainted with lessen overabundance data transfer capacity utilization. MD (Mediation Device) protocol is proposed to amplify the battery life of hubs in the MANET situation.

III. STUDIES AND FINDINGS

Dynamic Destination-Sequenced Distance-Vector Routing Protocol (DSDV) DSDV is developed on the basis of Bellman–Ford routing algorithm with some modifications. In this routing protocol, each mobile node in the network keeps a routing table. Each of the routing table contains the list of all available destinations and the number of hops to each. Each table entry is tagged with a sequence number, which is originated by the destination node. Periodic transmissions of updates of the routing tables help maintaining the topology information of the network. If there is any new significant change for the routing information, the updates are transmitted immediately. So the routing information updates might either be periodic or event driven. DSDV protocol requires each mobile node in the network to advertise its own routing table to its current neighbors.

Cluster Gateway Switch Routing Protocol (CGSR): CGSR uses DSDV protocol as the underlying routing scheme and, hence, it has the same overhead as DSDV. However, it modifies DSDV by using a hierarchical cluster-head-to-gateway routing approach to route traffic from source to destination. Gateway nodes are nodes that are within the communication ranges of two or more cluster heads. A packet sent by a node is first sent to its cluster head, and then the packet is sent from the cluster head to a gateway to another cluster head, and so on until the cluster head of the destination node is reached. The packet is then transmitted to the destination from its own cluster head.

Dynamic Source Routing (DSR): is a reactive protocol based on the source route approach. In Dynamic Source Routing (DSR), shown in, the protocol is based on the link state algorithm in which source initiates route discovery on demand basis. The sender determines the route from source to destination and it includes the address of intermediate nodes to the route record in the packet. DSR was designed for multi hop networks for small Diameters. It is a beaconless protocol in which no HELLO messages are exchanged between nodes to notify them of their neighbors in the network.

Ad Hoc on-Demand Distance Vector Routing (AODV): AODV is basically an improvement of DSDV but AODV is a reactive routing protocol instead of proactive. It minimizes the number of broadcasts by creating routes based on demand, which is not the case for DSDV. When any source node wants to send a packet to a destination, it broadcasts a route request (RREQ) packet. The neighboring nodes in turn broadcast the packet to their neighbors and the process continues until the packet reaches the destination. During the process of forwarding the route request, intermediate nodes record the address of the neighbor from which the first copy of the broadcast packet is received. This record is stored in their route tables, which helps for establishing a reverse path.

B. Use of Simulation software

There are numbers of software available which can mimic the process involved in your research work and can produce the possible result. One of such type of software is NS2. You can readily find NAM files related to research work on internet or in some cases these can require few modifications. Once these NAM files are uploaded in software, we can get the simulated results of paper and it easies the process of paper writing.

As by adopting the above practices all major constructs of a research paper can be written and together compiled to form a complete research ready for Peer review.

IV. CONCLUSION

MANET is part of networking that deal with mobile ad-hoc network. In the process of MANET different types of protocol have been utilized for realizable communication b/w the nodes mobile ad-hoc network has been connect b/w different nodes. These nodes communicate with each other without interference of any external architecture. Various types of attack have been performed in the MANET. That disrupts the performance of the overall network. These several attack have been done by malicious nodes available in the network. To overcome the issues of detection of malicious nodes in the network machines learning approach can be utilized that detect the malicious nodes on the basis of PDER, PMOR, and PMISR.

REFERENCES

[1] Priyanka Sharma "Enhanced Security Scheme against Jamming attack in Mobile Ad hoc Network", IEEE International Conference on Advances in Engineering & Technology Research, 2014, pp 22-30.

[2] Meenakshi Patel "Detection of Malicious Attack in MANET A Behavioral Approach", IEEE Conf. on Malicious attack, 2012, pp. 388-393.

[3] Ismail, Z., Hassan, R. "Effects of Packet Size on AODV Routing Protocol Implementation in Homogeneous and Heterogeneous MANET" Third International Conference on Computational Intelligence, Modeling and Simulation (CIMSiM), 2011, pp. 351 – 356.

[4] Thorat, S.A., Kulkarni, P.J. "Design issues in trust based routing for MANET" International Conference on Computing, Communication and Networking Technologies (ICCCNT), 2014,pp. 1 – 7.

[5] Durai, K.N., Baskaran, K. "Energy efficient random cast DSR protocol with mediation device in MANET" International Conference on Advanced Computing and Communication Systems (ICACCS), 2013, pp. 1 – 5.

[6] Sheikh, R., Singh Chande, M., Mishra, D.K. "Security issues in MANET: A review" Seventh International Conference on Wireless and Optical Communications Networks (WOCN), 2010, pp. 1 – 4.

[7] Rahman, F.M., Gregory, M.A. “4-N intelligent MANET routing algorithm” Australasian Telecommunication Networks and Applications Conference (ATNAC), 2011, pp. 1 – 6.

[8] Shah, N., Depei Qian “Cross-Layer Design to Merge Structured P2P Networks over MANET”16th International Conference on Parallel and Distributed Systems (ICPADS), 2010,pp. 851 – 856.

[9] Moradi, Z.,Teshnehlab, M., Rahmani, A.M. “Implementation of neural networks for intrusion detection in manet” International Conference on Emerging Trends in Electrical and Computer Technology (ICETECT), 2011, pp. 1102 – 1106.

[10] Capt. Dr. S. Santhosh Baboo and Mr. V J Chakravarthy, “An Improvement In Congestion Control Using Multipath Routing In MANET – Right Angled And Ant Search Protocol (RAAA)” The International Journal of Computer Science & Applications (TIJCSA), Volume 2,2010,pp. 45-49.

Publish Research Article

Dear Sir/Mam,

We invite unpublished Research Paper,Summary of Research Project,Theses,Books and Book Review for publication.

Address:- Dr. Ashak Hussain Malik House No-221, Gangoo Pulwama - 192301
Jammu & Kashmir, India
Cell: 09086405302, 09906662570,
Ph No: 01933212815
Email:- nairjc5@gmail.com, nairjc@nairjc.com , info@nairjc.com
Website: www.nairjc.com