iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 2 **Issue:** VII **Month of publication:** July 2014

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AN D ENGINEERING TECHNOLOGY (IJRASET)

A study of manet, attacks on it and defencing against packet dropping

Prof. Ajit Singh1, Neeraj Goyat2

1Dean, Department of Science And Information, Network Security2

B.P.S Mahila Vishwavidhalaya

Khanpur Kalan,Sonepat,India

Abstract— Mobile ad-hoc network is a self configuring infrastructure, rapidly deployable, less time consuming and a mobile networks , due to which it is applied in various fields. But there are number of attacks that affect the network transmission by dropping the packets. Not only the attacks, but also the network congestion is also the reason of packet drop during the communication. In this paper, we have studied about the manet, its applications, limitations, its security issues and all kind of attacks.

Keywords—MANET, Ad-hoc networks, Packet dropping attack, Attacks in Manet, Mobile ad-hoc networks,security issues, limitation in manet, application of manet.

INTRODUCTION

Manet (mobile ad-hoc network) is a kind of wireless network having free or autonomous node that are mobile and are self configurable, that is, they can operate by themselves. This network operates without stern top down network supervision. This network has no infrastructure. Cellular systems are less robust than Manet. The increment in the wireless devices or equipments such as Wi-Fi, 802.11 tablets or laptops have made Manet, an admired research topic. Manet can be connected to small internet as well as large internet. Manet has its routing networking setting on top of a link layer ad-hoc network.

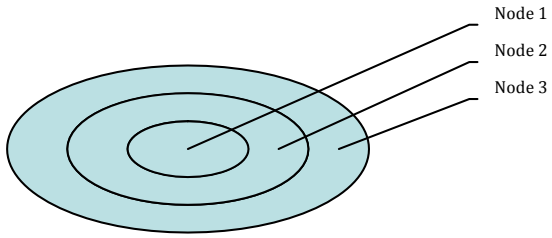


Fig 1: Ad-hoc (client to client)

In above figure, when nodes are set up to transmit in "ad hoc" mode, they create a wireless mesh network.

Manet can serve a number of applications such as:-

- Commercial environment e.g. electronic payments from everywhere,
- business,
- military,

ISSN: 2321-9653

- customers in industries such as emergency/disaster response, homeland security, mining, industrial monitoring,
- Mine site operations,
- Police exercises,
- Robot data acquisition
- Vehicular services etc.

It is used in various fields due to following reasons:-

- Rapid deployable
- Self configurable
- Mobility
- Infrastructure-less
- Cost effective
- Less time consuming
- More robust than cellular system
- Decentralized network
- Multi-hop
- Power constraint
- Variation in scale
- Heterogeneity

But there are some limitations of Manet. They are:-

- Deficient of resources:- which raise the problem of security
- Deficiency of services for authorization.
- Topology varies from time to time due to which it become hard to find the malicious site.
- The protocols which are used for fixed infrastructure cannot be applied to Manet.

SECURITY ISSUES

Now a day, it's a trend to have a wireless, movable, infrastructure less, compact and slim system. Because of these reasons, the mobile Network has become one of busiest public ad-hoc network. And due to its applicability in almost every field, and absence of fixed infrastructure it become difficult to make use of the existing routing technique for network services and this posses a number of challenges in ensuring the security of communication. There are many issues or challenges that are needed to be considered when an ad-hoc network is created. These issues may be:-

- Routing
- Multicasting
- Medium access scheme
- Absence of infrastructure
- Pricing scheme
- Security
- Power and computation limitation
- Self organization
- Node vulnerability
- Energy management
- Scalability
- Channel vulnerable
- Deployment considerations etc.

One of such issue is the security issue. In ad-hoc network security of network such as shared wireless medium, open peer-to-peer network architecture, stringent resource constraints, and highly dynamic network topology etc becomes

ISSN: 2321-9653

much more difficult than the wired networks. There are number of attacks that affect the network communication by dropping the packets. Not only the attacks, but also the network congestion is also the reason of packet drop during the communication.

SECURITY ATTRIBUTES

Security attributes can be considered as:-

a. Availability: It ensures that network is surviving despite of denial of service attack.

b. Authentication: when a node is communicating with any other peer node, than it enables the node to identify the peer node.

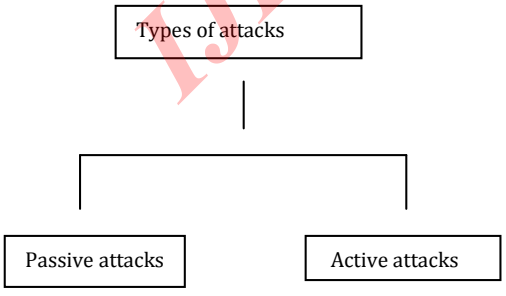
c. Non repudiation: It ensures that the sent message is original.

d. Confidentiality: It ensures that the unauthorized devices are not able to receive the secret data.

e. Integrity: It ensures that the receiver should not receive the corrupted data.

TYPES OF ATTACK

The classification of intrusion makes us easy to find the menace severity and makes easy to provide explication to them. We have classified these attacks into two categories.



Passive attacks:-

Passive attacks are those attacks which do not change any data or message in the network but these attacks, that is, unauthorized site or node only listen to the network and, are able to know the confidential or secret data. Theses malicious nodes or sites are difficult to detect because they do not affect the network traffic or data. To avoid these kinds of attacks a strong encryption algorithm to encrypt the data can be used while transmitting the message or data.

Active attacks:-

Active attacks are the attacks which disturb the Manet network by preventing the data flow from source node to destination node. These attacks can be done either from internal site or from external site. These attacks create the unauthorized access which helps the malicious node to alter, modify, delete, and create the data between the source and destination node. The internal attacks are more difficult to detect than external attacks.

Internal Packet Dropping attack

This type of Packet Dropping attack has an internal malicious node which fits in between the routes of given source and destination. As soon as it gets the chance this malicious node make itself an active data route element. At this stage it is now capable of conducting attack with the start of data transmission. This is an internal attack because node itself belongs to the data route. Internal attack is more vulnerable to defend against because of difficulty in detecting the internal misbehaving node.

External Packet Dropping attack

ISSN: 2321-9653

External attacks physically stay outside of the network and deny access to network traffic or creating congestion in network or by troublemaking the entire network. External attack can become a kind of internal attack when it take control of internal malicious node and control it to attack other nodes in WMN. External Packet Dropping attack can be summarized in following points

- Malicious node detects the active route and notes the destination address.
- Malicious node sends a route reply packet (RREP) including the destination address field spoofed to an unknown destination address. Hop count value is set to lowest values and the sequence number is set to the highest value.
- Malicious node send RREP to the nearest available node which belongs to the active route. This can also be send directly to the data source node if route is available.
- The RREP received by the nearest available node to the malicious node will relayed via the established inverse route to the data of source node.
- The new information received in the route reply will allow the source node to update its routing table.
- New route selected by source node for selecting data.
- The malicious node will drop now all the data to which it belong in the route.

In AODV Packet Dropping attack the malicious node "A" first detect the active route in between the sender "E" and destination node "D". The malicious node "A" then send the RREP which contains the spoofed destination address including small hop count and large sequence number than normal to node "C".

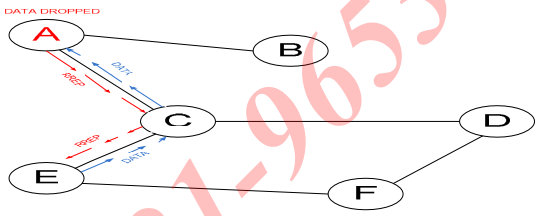


Figure: 1 Packet Dropping attack specification

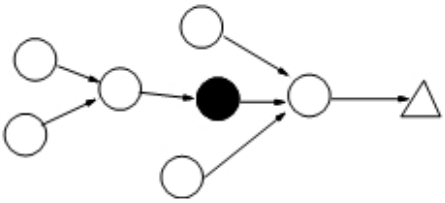
This node "C" forwards this RREP to the sender node "E". Now this route is used by the sender to send the data and in this way data will arrive at the malicious node. These data will then be dropped. In this way sender and destination node will be in no position any more to communicate in state of Packet Dropping attack.

In the fig:2 we shown how many ways an adversary can deploy malicious nodes in transmission path to BS. Fig 2(c) shows how all the nodes surrounding base station are compromised. Note that in this case, base station does not receive any message and none of the countermeasures work. Physically the network has to be redeployed.

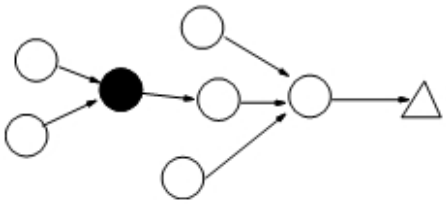
Based on its selection in packet drops, selective Packet Dropping can be classified into two types:

- Drops packets of some specified nodes
- Drops packets of some specified type

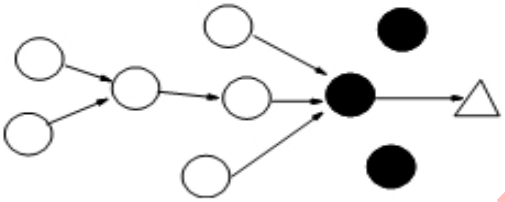
ISSN: 2321-9653



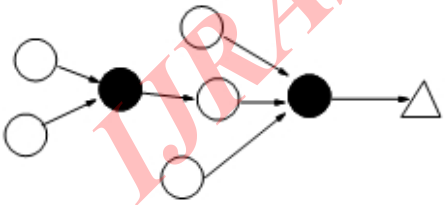
(a) Single Malicious Node



(b) Two Consecutive Malicious Node



(c) Surrounding Malicious Nodes



(d) Non Consecutive Malicious Nodes

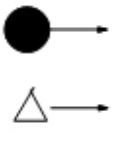


Figure2: Categorization Of Selective Packet Dropping Attack based on malicious node count in network

Here are some of the attacks that have been explained.

Wormhole

In the wormhole attack an adversary tunnels mail received in one part of the network over a low latency link and replays them in a diverse part. An adversary situated close to a base station may be able to completely interrupt routing by creating a well-placed wormhole. An adversary could persuade nodes who would normally be multiple hops from a base station that they are only one or two hops away via the wormhole. This can craft a sinkhole: since the adversary on the other side of the wormhole can artificially provide a high-quality route to the base station, potentially all traffic in the surrounding area will be drawn through her if alternate routes are significantly less attractive.

Sybil

Sybil attack is defined as a "malicious device illegitimately taking on multiple identities". Using the Sybil attack, an adversary can "be in more than one place at once" as a single node presents multiple identities to other nodes in the network which can significantly reduce the effectiveness of fault tolerant schemes such as distributed storage, disparity and multi path. It may be extremely difficult for an adversary to launch such an attack in a network where every pair of adjacent nodes uses a unique key to

initialize frequency hopping or spread spectrum communication. Sybil attacks also pose a significant threat to geographic routing protocols.

Acknowledgement Spoofing

Several sensor network routing algorithms rely on implicit or explicit link layer acknowledgements .Due to the inherent broadcast medium, an adversary can spoof link layer acknowledgments for overheard packets addressed to adjoining nodes. Goals include convincing the sender that a weak link is strong or that a dead or disabled node is alive.

Traffic Analysis

Traffic analysis attacks are forged where the base station is determinable by observation that the majority of packets are being routed to one particular node. If an adversary can compromise the base station then it can render the network useless

Selective Packet Dropping Attack

In a selective Packet Dropping attack malicious nodes behaves like black hole and may refuse to forward certain messages and simply drop them, ensuring that they are not propagated any further. However, such an attacker runs the risks that neighboring nodes will conclude that she has failed and decide to seek another route. A more subtle form of this attack is when an adversary selectively forwards packets. An adversary interested in suppressing or modifying packets originating from a few selected nodes can reliably forward the remaining traffic and limit suspicion of wrong doing.

REFERENCES

[1] Amey Shevtekar," Do Low Rate DoS Attacks Affect QoS Sensitive VoIP Traffic?", IEEE ICC 2006, 1-4244-0355-3/06@ 2006 IEEE

[2] Djamel Djenouri," On Securing MANET Routing Protocol Against Control Packet Dropping", 1-4244-1326-5/07@2007 IEEE

[3] S. Yi, P. Naldurg, and R. Kravets, Security Aware Ad hoc Routing for Wireless Networks. Report No.UIUCDCS-R-2002-2290, UIUC, 2002

[4] H. Luo and S. Lu, URSA: Ubiquitous and Robust Access Control for Mobile Ad-Hoc Networks, IEEE/ACM Transactions on NetworkingVol.12 No.6(2004) pp. 1049-1063.

[5] W. Lou and Y. Fang, A Survey of Wireless Security in Mobile Ad Hoc Networks: Challenges and Available Solutions.Ad Hoc Wireless Networks, edited by X. Chen, X. Huang and D. Du. Kluwer Academic Publishers, pp. 319-364,2003.

[6] Bing Wu, Jianmin Chen, Jie Wu, Mihaela Cardei: A Survey on Attacks and Countermeasures in Mobile Ad Hoc Networks. Wireless/mobile network security Y. Xiao, X. Shen, and D.-Z. Du (Eds.) pp. – - –2006 Springer

[7] Nishu Garg, R.P.Mahapatra. “MANET Security Issues”. IJCSNS International Journal of

Computer Science and Network Security,

Volume.9, No.8,2009.

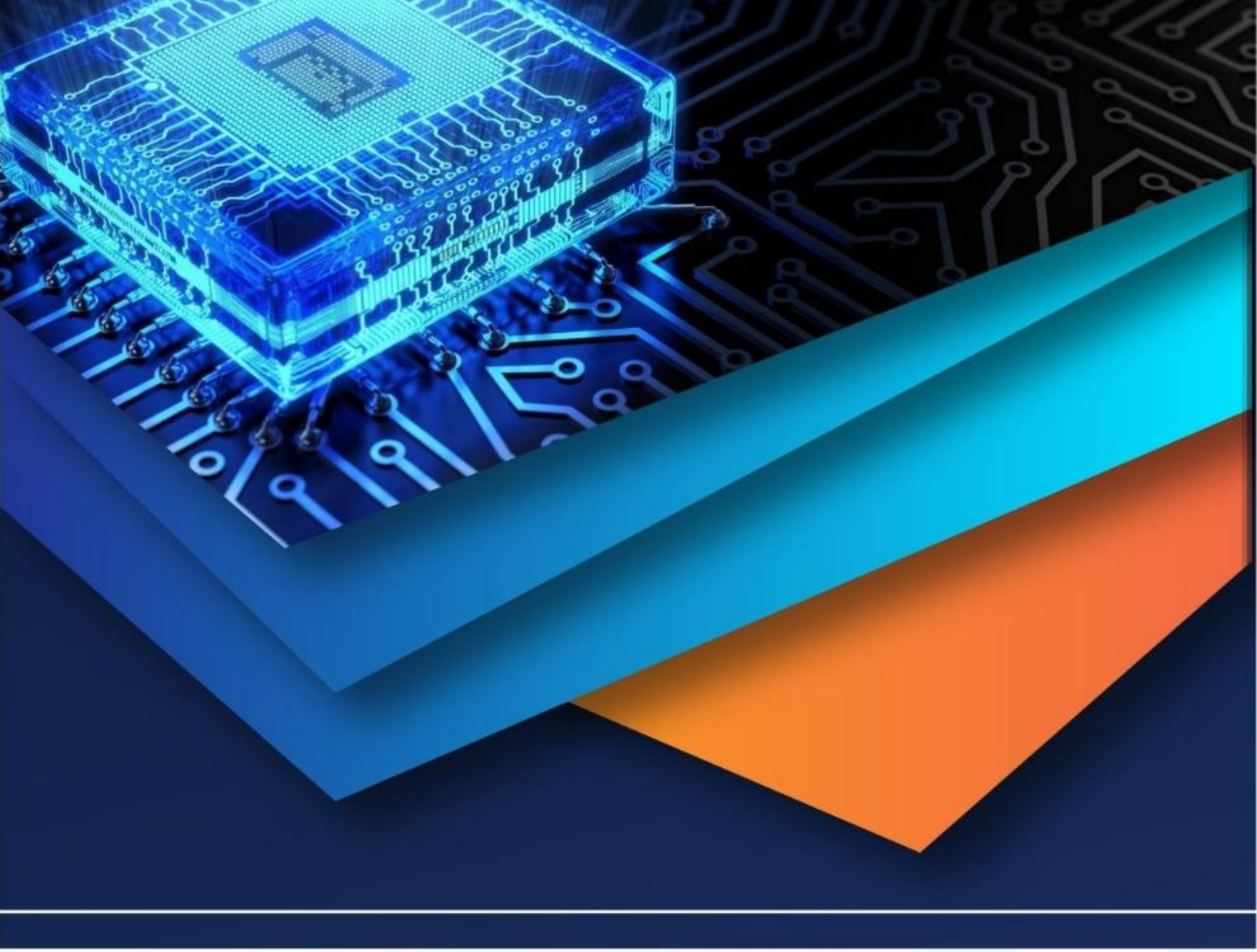
[8] F. Kargl, A. Geiß, S. Schlott, M. Weber. "Secure Dynamic Source Routing". Hawaiian International Conference on System Sciences 38 Hawaii, USA, January 2005.

[9] rushu nandy and Debdutta Barman Roy. "Study of Various Attacks in MANET and Elaborative Discussion Of Rushing Attack on DSR with clustering scheme. Int. J. Advanced Networking and Applications Volume: 03, Issue: 01, Pages:1035-1043 (2011)

[10] ihye Kim, Gene Tsudik. "SRDP: Secure route discovery for dynamic source routing in MANET's".Ad Hoc Networks, Volume 7, Issue 6,Pages 1097-1109, August 2009.

[11] Bin Xie and Anup Kumar. "A Framework for Internet and Ad hoc Network Security". IEEE Symposium on Computers and Communications (ISCC-2004), June 2004.

[12] J. Broch et al., "A performance comparison of multi-hop wireless ad hoc network routing protocols" in ACM Mobicom '98, Oct. 1998.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY