# Review Paper on Impact of Attacks on MANET

Manpreet Kaur[1], Er. Manoj Kumar[2]

*M.Tech student[1], Assistant Professor[2]*

*Department of Computer Engineering, YCOE, Punjabi University, Patiala Guru Kashi Campus, Talwandi Sabo, Punjab*

***Abstract:*** **MANET is infrastructure less and freelance network that consist varied nodes. MANET is mobile spontaneous network having ability to attach varied mobile nodes to every alternative. These nodes use wireless links to speak with one another. This temporary, low price network will connect little space folks, because it is temporary infrastructure less, having less variety of resources like low security live, low node life time and fewer authentication suggests that. The infrastructure less nature of painter makes it susceptible to varied attacks. Attacks square measure prone to occur if detective work and preventing algorithms fails to sight vulnerable threats and to seek out and take away malicious nodes. Thus, in MANET, attacks square measure significantly serious issue. during this paper, we've examined sure attacks in painter. Finally, we've compared some attacks exploitation some necessary parameters so self-addressed impact of attacks.**

## I. INTRODUCTION

A mobile circumstantial network may be a network that's fashioned by assortment of 2 or additional nodes (devices) that moves in random manner. One node will communicate with another that's inside its radio vary or outside their radio vary. It follows AN infrastructure less design nevertheless features a potential of service discovery, routing and packet forwarding. Communication is feasible between 2 nodes with the assistance of routing protocols. In these varieties of networks nodes will move willy-nilly from one place to a different while not maintaining any topology, no static topology is there. At any time they'll be a part of the network and leave the network. These networks is simply deployed and additionally setup time is extremely less as a result of they are doing not have mounted infrastructure.

## II. ATTACKS CLASSIFICATION

Attacks are often classified in several classes like internal attacks, External attacks, Active Attacks Passive Attacks. Aggressor will damage the network as internal, external or active; passive therefore this classification is incredibly necessary.

### *2.1 External Attack*

These attacks area unit primarily utilized by the one who is outside the network and wish to urge access to the network.

And if they get entry to the network then they misuse it, they send spoofed packets and thanks to that the full network gets down. In wired network this attack is additionally there. It are often prevented with the assistance of firewalls [3].

### *2.2 Internal Attack*

This attack is typically happens within the network. The aggressor will commonly involve within the communication. a brand new node that's more to the network will act as associate degree aggressor that has gain the access to a network. it's gain access to the network either by creating a affect current node or by impersonation. it's terribly troublesome to predict the interior attacks as compared to external attack [3].

### *2.3 Passive Attacks*

In this attack, associate degree aggressor solely listens or keeps track info} or information that's being transferred between 2 parties. No modification and fabrication is completed. samples of passive attacks area unit eavesdropping and Traffic Analysis. Attackers will simply get all the data regarding the network that's helpful in hijacking or injecting associate degree attack within the network. it's quite exhausting to discover passive attacks as compared to active attacks.

### *2.3.1 Eavesdropping*

In this the offender listen all knowledge} that's being transmitted between the 2 parties so as to search out some helpful data like passwords, secret codes, direction etc.

### *2.3.2 Traffic Analysis*

In this the offender keeps track of the traffic flow so he's able to observe the situation of the hosts. By exploitation this methodology the offender will confirm the patterns, frequency and length of the message.

### *2.4 Active Attack*

In active attack the attackers modify the info. it's essentially wont to scale back the performance of the network. a number of the samples of active attacks area unit masquerade attacks, replay attacks, DOS attacks.

### *2.4.1 SYBIL ATTACK*

A Sybil attack may be a scenario wherever a malicious node acts like 2 or additional nodes instead of simply a node like antecedently mentioned attacks [10]. The Sybil nodes square measure created by series of false identities, imitations, or impersonation of nodes in a very Manet, and these further node identities may be generated by simply a physical device. The assaulter tries to act as many totally different identities or nodes instead of one [11]. Work on analyzing the doable Sybil attack victimization mathematical approach shown that the validity of Sybil attacks [12].

### *2.4.2. BLACKHOLE ATTACK*

Blackhole attack issues with the network layer of MANET. In region attack, associate in Nursing assaulter or malicious node aims to consume all the information packets throughout the network. Region attack is often of various varieties reckoning on aims of the assaulter when interception of information exchange between alternative nodes. Reckoning on region kind, when interception of information exchange assaulter will either drop all the packets [1] or it will by selection drop packets, or maybe the malicious node will modify the packets.

### *2.4.3. Warmhole ATTACK*

The hole attack is one in every of the foremost severe attacks of Manet. hole attack may be a form of the Denial-of-Service attacks effective on the network layer. It affects network routing, and particularly location based mostly wireless security [14]. The whole attack is largely launched by a combine of collaborating nodes. In whole attack 2 collaborating assaulter nodes occupy robust strategic locations in 2 totally different components of the network. By occupying dominant positions in a very network these 2 nodes will cowl complete network and advertise to possess the shortest path for transmittal information. The 2 assaulter nodes square measure connected to every alternative employing a link that is termed hole tunnel. At one finish of hole tunnel, one node overhears the packets in its native space and forwards them to the opposite node that replays them to its native space.

## III. Related Work

Singh et al. presents Mobile Ad-Hoc Networks (MANET) is becoming a popular research area among researchers due to its versatile routing nature. Routing in MANET is a challenging issue due to dynamic network topology, limited bandwidth and limited battery power. Attacks are liable to occur if routing algorithms fails to detect vulnerable threats and to find and remove malicious nodes. Thus, in MANET, collaborative attacks are particularly serious issue. In this paper, we have examined certain collaborative attacks in MANET. Finally, we have compared some attacks using some important parameters and then addressed major issues related to this.

Upadhyay et al. presents In this paper, we discuss the impact of wormhole attack in MANETs. The wormhole attack is difficult to detect by using any cryptographic measures because they do not create any separate packets. In this work, several techniques of wormhole detection like watchdog, nodes with directional antenna and cluster based approach etc. Some prevention techniques such as packet leashes, time-of-flight, delphi protocol, pathrater technique etc. are also presented. The result analysis shows the impact of wormhole attack on MANETs in terms of throughput variations.

Garg et al. presents there is an attack which causes many serious threats to the network and it is known as Sybil attack. In Sybil attack, attackers or malicious nodes uses many identities or IP addresses to gain control over the network and creates lots of misconception among nodes present in the network. In this paper two approaches are discussed to detect the Sybil Attack, one is Lightweight Sybil Attack Detection Approach and other is Robust Sybil Attack Detection Approach.

Parsons et al. In this paper we implement and evaluate the most prominent attacks described in literature in a consistent manner to provide a concise comparison on attack types and parameters. Our objective is to thoroughly capture and analyze the impact of a range of attacks on MANET performance. To this end we define performance metrics and explore influence and damage caused by several attack types and parameter sets. Our evaluation results show that the degree of impact of attacks differs significantly depending on attack type and parameters used. The impact of a particular attack increases considerably with an increasing number of attacking nodes in several of the scenarios, whereas other attack impact levels remain almost constant with varying number of attackers.

Mohebi et al. In this paper, two routing protocols (AODV and DSR) are simulated under regular operation, single and cooperative black hole attack. This work has been performed by simulator to show consequence of black hole attacks in MANET by using various graphs which are used to collect data in term of several metrics. One common method to perform most of researches in the MANET security field is to simulate and analyze the routing protocols in various scenarios.

Kasiran et al. presents In order to communicate each other, the nodes cooperatively forward data packets to other nodes in the network by using the routing protocol. However, these routing protocols are not secure hence leaving the MANET unprotected from malicious attack. Wormhole attack is a common malicious attack in MANET environment. The network consisting of 20, 60 and 100 mobile nodes uses the random model in 1000m x 1000m flat area. The sources are spread randomly over the network and only 512 bytes data packets are used. Each packet is uniformly dispersed at 180 sec, starting its journey from a random location to a random destination the objective of this paper is to evaluate the throughput performance in AODV with the existence of wormhole and Sybil attack.

Patidar et al. The paper proposes protocols which will protect ad hoc networks from Blackhole and wormhole attacks and to improve network stability. This paper presents an intrusion detection system based on the concept of specification-based detection system to detect and prevent blackhole attacks. This paper also presents a hop count analysis approach to detect wormhole attacks along routes in ad hoc networks. The proposed protocol does not require any location information, time synchronization, or special hardware to detect wormhole attacks.

## IV. IMPACT OF ATTACKS

| Attacks | Attacks Category | Packet lose | Battery Power | Goals | Layer |
|---|---|---|---|---|---|
| Sybil | Active | 30% possibility | Medium | Droping packets | Muti Layer |
| Warm hole | Active | 40% possibility | Medium | Wrong packets | Network Layer |
| Black hole | Active | 50% possibility | High | Droping packets | Network Layer |
| Evase droping | Passive | No lose | Low | Accessing Packets | Physical Layer |
| Traffic Analysis | Passive | No lose | Low | Accessing Packets | Data link Layer |

## V. CONCLUSION

these days everybody has laptops, Smartphone's, PDA's and that they wish to attach these devices with others device so they will exchange info and Manet is that the solely answer to that. it's temporary network that is about informed the temporary basis and disconnected once the work has been done. it's higher for little space solely. it's nice applications within the field of military, hospitals (fast retrieval of data), education (virtual lecture rooms, conferences), emergency (disaster, earthquake). Sensors area unit little device that area unit deployed in a very specific area unit for sensing {the data|the info|the info} or information. small sensors area unit employed in military, health industries, food industries, used for environmental and weather military operation. however it's conjointly true that this network is at risk of many attacks i.e. security is that the major issue in wireless network. thence this paper shows differing kinds of attacks in Manet. This paper centered on active attacks like region, Wormhole, Sybil attack and passive attacks.

## REFERENCES

[1]. S. Upadhyay and B. K. Chaurasia, "Impact of Wormhole Attacks on MANETs", 2011, vol. 2, Issue 1.

[2]. R. Garg, H. Sharma," Comparison between Sybil Attack Detection Techniques: Lightweight and Robust" in International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering, 2014, Vol. 3, Issue 2.

[3]. M Parsons, P. Ebinger, "Performance Evaluation of the Impact of Attacks on Mobile Ad hoc Networ" in International Conference on Computer Science and Electronics Engineering, 2015, pp. 339-342.

[4]. Z. Kasiran and J. Mohamad, "Throughput Performance Analysis of the Wormhole and Sybil Attack in AODV" .

[5]. J. Gnanambigai, N. Rengarajan and K. Anbukkarasi, "Leach And Its Descendant Protocols: A Survey" International Journal of Communication And Computer Technologies, 2012, vol. 3, pp. 15-21.

[6]. K. Patidar, V. Dubey, "A Comparative study of Collaborative Attacks on Mobile AdHoc Networks" International Journal of Emerging Technology and Advanced Engineering, 2014, vol. 4, Issue 8.

[7]. K. Patidar, V. Dubey, "Modification in Routing Mechanism of AODV for Defending Blackhole and Wormhole Attacks" International Journal of Advanced Research In Computer And Communication Engineering, 2014, vol. 3, pp. 5683-5690.

[8]. Y.-C. Hu, A. Perrig, D. B. Johnson, "Wormhole Attacks in Wireless Networks, Selected Areas of Communications," in IEEE Journal on, vol. 24, no. 2, pp.370-380, 2006

[9]. A. Nadeem and M. P. Howarth,``A survey of MANET Intrusion Detection & Prevention Approaches for Network layer Attacks," IEEE Communication Surveys & Tutorials, 2012, pp.1-19.

[10]. J,HeeCho,A. Swami,and Ing-Ray Chen,``A Survey on Trust Management for Mobile Ad Hoc Networks for Mobile Ad-Hoc Networks, 2011,"IEEE Communication Surveys & Tutorials, Vol.13, No.4, pp.562-583.

[11]. B. Wu, J. Chen, J. Wu and M. Cardei, "A Survey on Attacks and Countenneasures in Mobile Ad Hoc Networks", Wireless/Mobile Network Security, Springer,2006.

[12]. Y. F. Alem and Z. C. Xuan, "Preventing Black Hole Attack in Mobile Ad-hoc Networks Using Anomaly Detection", 2nd International Conference on Future Computer and Communication, IEEE, Vol. 3, pp 672-676, 2010.

[13]. L. Qian, N. Song and X. Li, "Detecting and Locating Wormhole Attacks in Wireless Ad Hoc Networks through Statistical Analysis of Multi-path", IEEE Wireless Communications and Networking Conference, Vol. 4, pp 2106-2111,2005.