A Proactive Approach to Secure MANET using an Intrusion Detection System

Farhin Shaikh
M.Tech, Raksha Shakti University, Ahmedabad, Gujarat, India
Chandresh Parekh
Assistant Professor, Raksha Shakti University, Ahmedabad, Gujarat, India

ABSTRACT: The MANETs are a kind of Ad Hoc network and is used for mobile communication. The ad hoc mobile Networks (MANETS) are used when the user moves. MANET does not depend on established infrastructure. MANETs use wireless networks to connect to different networks. The self-configuring capability in MANET is absolutely critical to key mission applications such as military use or disaster recovery. The mobility and scalability offered by wireless network have made it possible in many applications. Surrounded by the latest mobile networks, Mobile Ad-hoc Network (MANET) is one of the most popular significant and exclusive applications. There is an increasing threat of attacks on the MANET because of vulnerabilities of wireless links, periodic nature of connectivity, changing topology etc. Security is the main concern in the MANET. As a result of the dynamic infrastructure less nature and decentralized networks, wireless Ad-hoc networks are unprotected and vulnerable to the attack. This paper focuses on the study of the black hole attack. In this paper detection and prevention techniques of black hole attack are implemented in MANET routing protocol namely AODV as reactive routing protocol. Black hole attack is one of the security hazard in which the traffic is redirected to malicious node that actually does not exist in the network. My literature survey is to understand different attacks on MANET like Black hole attack, Wormhole attack, Grey hole attack, Flooding attack, Denial of Service (DOS) etc. And Study the related work in MANET security. From that I have to implement efficient detection technique for Black hole attack.

Keywords: Mobile Ad-Hoc Networks (MANETs), Intrusion Detection System (IDS), Black hole attack, AODV.

I. INTRODUCTION

Versatile Ad hoc NETwork (MANET) is a gathering of portable hubs collected with both a remote transmitter and a recipient that speak with each other by means of bidirectional remote connections either straightforwardly or in a roundabout way. MANET does not require a settled foundation; along these lines, all hubs are allowed to move arbitrarily. MANET can making a self-designing and self-keeping up arrange without the assistance of a concentrated framework. MANET is winding up increasingly widely executed in the business [3] [13].

One of the significant focal points of remote systems is its capacity to permit information correspondence between various gatherings and still deal with their versatility. In any case, this correspondence is restricted to the territory of transmitters. This implies two hubs can't contact with each other when the separation between the two hubs is past the correspondence region of their own. In opposing to the customary remote system, MANET has decentralized system framework. MANET does not require a settled framework; along these lines, all hubs are allowed to move arbitrarily. MANET can making a self-designing and self-keeping up organize without the assistance of a unified framework, which is regularly unavailable in basic mission applications like military clash or crisis recuperation. MANET is organized to be utilized as a part of crisis conditions where a foundation is difficult to reach or difficult to introduce in situations like common or human-instigated calamities, military clashes, and medicinal crisis conditions [3] [13].

MANETs have numerous applications in different fields. For instance, they have been utilized as a part of a military setting since the 1970s to guarantee the opportune stream of data and order in fight, adding to the achievement of a mission. MANETs are likewise perfect for balancing out correspondence organizes and giving salvage administrations following catastrophic events, for example, tremors or surges [6].

II. BACKGROUND

Attacks in MANETs

Numerous kinds of assaults should be possible through a MANET.

Classification of Attacks in MANETs

MANETs can be partitioned into two primary classes, in particular aloof assaults and dynamic assaults. Aloof assaults are normally simply dropping information, while dynamic assaults include activities by enemies, for example, replication, adjustment, and erasure of traded information.

1) **Passive Attacks:** MANETs are more powerless against uninvolved assaults. A uninvolved assault is a system assault in which a framework is checked and here and there scanned for open ports and vulnerabilities. Uninvolved assaults incorporate unapproved listening in on organize movement or gathering information from arrange activity. Uninvolved assaults are performed to take important data in the goal systems. Cases of latent assaults in the impromptu system are listening stealthily and activity assaults. Recognizing this sort of assault is basic in light of the fact that neither the framework assets nor the basic system capacities are physically harmed to demonstrate the interruptions [8].

Eavesdropping

An interruption in which somebody tries to take data that PCs, cell phones, or different gadgets transmit over a system. A listening stealthily utilizes unsecured system interchanges to get the transmitted and got information.

Location Disclosure Attack

In this assault, the security necessities of a hub are bargained. By utilizing an activity examination method or with easier testing and observation approaches, an assailant can decide an area of the hub and the structure of the system [9].

Traffic Analysis

In MANETs both the information bundles and activity designs are imperative to aggressors. For instance, classified data about the system topology might be inferred by dissecting activity designs. Movement investigation can likewise be executed as a dynamic assault by wrecking hubs, which empowers arrange self-association, and important topology information can be gathered.

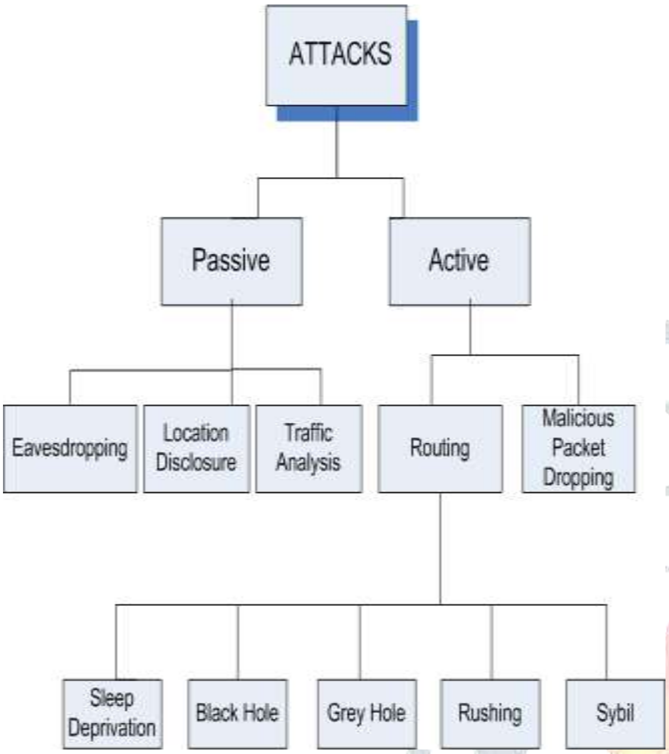

Fig 1: - Classification of Attacks in MANETs

2) Active Attacks: Active assaults are intense assaults on the system that stop the stream of messages between the hubs. These assaults make unapproved access to the system, which enables the aggressor to roll out improvements, such as, evolving bundles, changing and erasing traded information, message retries, and message creation, and foreswearing of-benefit assaults, replication [8].

Black hole Attack

Dark gap assault is the significant issue for the MANET, where a pernicious hub conveys erroneous directing data, expressing that it offers the most limited way for the goal hub whose parcels it needs to hinder and after that confine without achieving its goal [7].

Gray hole Attack

Dim gap assault is the sort of dynamic assault that prompts the dropping of the information parcels. The pernicious hub right off the bat licenses to transmit the parcels and after that neglects to do as such [7]. Dark gap assaults make the interloper hub to communicate the comparative activity as a bona fide hub amid disclosure of course, which prompts dropping of bundles from specific hubs [10].

Sleep deprivation attacks

This sort of assault is in reality more particular to the portable specially appointed systems. The point is to deplete off restricted assets in the versatile specially appointed hubs (e.g. the battery powers), by continually makes them occupied with handling pointless bundles. In a steering convention, lack of sleep assaults may be propelled by flooding the focused on hub with superfluous directing bundles. For example, aggressors could surge any hub in the systems by sending countless demand (RREQ), course answers (RREP) or course blunder (RERR) bundles to the focused on hub. Accordingly, that specific hub can't take an interest in the directing instruments and rendered inaccessible by alternate hubs in the systems [8].

Rushing Attack

It utilizes counterfeit concealment amid the course revelation process inclined to this assault. An aggressor who can transmit more course asks for quicker than genuine hubs can improve the probability that the courses contain the assailant rather than the valid course, the loud assault anticipation offers the guard against the assault [10].

Sybil Attack

Every hub in a specially appointed portable system looks for a critical deliver to partake in directing, and hubs are distinguished by the address on the system. There is no focal specialist to check these characters in MANETs. An assailant can exploit this component and assessment bundles, such. RREQ or RREP, with various personalities. This is called Sybil assault [10].

Malicious Packet Dropping

In this kind of assault, parcels are disposed of without cause. This parcel dropping at a vindictive middle of the road hub may bring about an intrusion in the correspondence or age of false data between the source and the goal, which is a bothersome circumstance.

3) External assaults: External assaults are assaults propelled by adversaries who are not at first approved to take an interest in organize tasks. Ordinarily, these assaults are expected to cause arrange blockage, deny access to certain system includes, or upset all system activities. Counterfeit Packet Injection, Denial of Service, and Impersonation are only a portion of the assaults typically started by outside assailants [8].

4) Internal assaults: Internal assaults are started by the approved hubs in the systems and may originate from traded off and malevolent hubs. Inward hubs are assigned as traded off hubs when the outer assailants have captured the approved inside hubs and after that utilization them to dispatch assaults against the specially appointed systems. Security prerequisites, for example, confirmation, secrecy, and respectability are greatly powerless in the specially appointed systems with the traded off inner hubs, since the correspondence keys utilized by these hubs might be stolen and sent to the next clashing aggressors [8].

III. AODV PROTOCOL

Every hub in an impromptu system keeps up a directing table that contains data about the course to a particular goal. At whatever point a bundle is to be sent by a hub, it first checks with its directing table whether a course to the goal is as of now accessible. Provided that this is true, it utilizes this course to send the parcels to the goal. In the event that a course isn't accessible or the already entered course is crippled, the hub starts a course revelation process.

A RREQ (Route REQuest) bundle is sent by the hub. Every hub that gets the RREQ parcel first verifies whether it is the goal for that bundle, and in the event that it does, it sends back a RREP (Route Reply) bundle. In the event that it isn't the goal, it checks with its directing table in the event that it has a course to the goal. If not, it advances the RREQ parcel by sending it to its neighbors. On the off chance that its steering table contains a passage to the goal, at that point the subsequent stage is to analyze the "goal grouping" number in its directing table with the one present in the RREQ bundle. This goal arrangement number is the succession number of the last sent parcel from the goal to the source. In the event that the objective arrangement The number in the steering table is not exactly or equivalent to the number contained in the RREQ bundle, at that point the hub advances the demand to its neighbors. In the event that the number in the steering table is more noteworthy than the number in the bundle, this shows the course is a "crisp course" and parcels can be sent over that course. This middle of the road hub at that point sends a RREP parcel to the hub through which it got the RREQ bundle. The RREP parcel is come back to the source by means of the invert course. The source hub at that point refreshes its steering table and sends its parcel over that course. Amid the task, when a hub recognizes an association mistake, it sends a RERR (Route ERRor) bundle to every other hub that utilization that association with speak with different hubs [11].

IV. BLACKHOLE ATTACK

Dark Hole is considered as an inner assault in Network Layer and is elusive, as even malignant hubs make a ton of harm the system. A dark gap hub sends fashioned directing data and cases that it has an ideal course to the goal asked for by the source hub and educates other great hubs to course information parcels through it and expend the transmitted bundles [12]. A dark opening assault is a sort of dissent of administration assault in which a pernicious hub can pull in all parcels by erroneously asking for another course to the goal and after that engrossing it without passing it on to the goal [11]. ,

V. PROPOSED WORK

AODV is responsive steering convention. AODV is a receptive directing convention. For the security of MANET, we have utilized our proposed work in to the AODV steering convention. In this work, we propose a discovery and avoidance strategy against dark gap assaults. These methods depend on the accompanying calculation.

Stage 1: select one transmitting hub and a getting hub
Stage 2: Deliver Acknowledgment to every hub of the system.
Stage 3: Wait for Acknowledgment back to Source hub.

Stage 4: List typical hubs without dark opening assaulted hubs.
Stage 5: Set the most limited way to exchange the information from the source to goal.
Stage 6: When exchanging information
In the event that dark opening hub at that point
Take after stage 5 until the point that way is found without

Dark opening hub.

Stage 7: wrap up
Stage 8: for aversion boycotts that utilization every single noxious hub and not later on.

VI. IMPLEMENTATION

To assess the execution of the proposed calculation, we utilized NS-2 (v-2.35) organize test system. The re-enactments were performed with an Intel (R) Core (TM) I5 processor at 2.40 GHz, 4 GB of RAM running Ubuntu 16.04 Linux. We utilize the IEEE 802.11 calculation at the physical/information connect layer. We utilize standard AODV responsive steering calculation at arrange layer. At last, client datagram convention (association less) is utilized at the vehicle layer. The landscape territory is 1186m X 584m with 25 hubs changing from 10 to most extreme 90 at various rates from 10 m/s to 90 m/s.

Essential parameters utilized for experimentation. A portion of the tests that have been directed to check the conduct of the AODV convention under dark opening assaults are recorded underneath:

Examined protocols	AODV
Simulation time	1000 seconds
Number of Nodes	25
Number of malicious node	2
Traffic Type	TCP
Performance Parameter	Throughput, delay, Packet Delivery Ratio
Pause time	100 seconds
Mobility (m/s)	10 meter/second
Packet Inter-Arrival Tim	exponential(1)
Packet size (bits)	exponential(1024)
Transmit Power(W)	0.005
Date Rate (Mbps)	11 Mbps
Mobility Model	Random waypoint

Usage

Concurring our proposed work we begin our execution by making dark opening assault utilizing AODV convention in Network Simulator 2.35.

Initially Install NS2 in Linux UBUNTU 16.04 and furthermore introduce Network Animation.

Making Black opening Attack in AODV: For making Black gap assault in to AODV we utilize 25 hubs. Here hub 20 and 21 are the source hubs, and hubs 9 and 17 are the goal hubs.

In this system hub 1, 7 and 13 are the dark gap hub. It advances the bundles to another hub.

We utilize the AODV convention and different wordings to help us to decide the dark opening in the system.

A dark gap hub 7 sends manufactured steering data, guaranteeing to have an ideal course to the goal asked for by the source hub, and educates other great hubs to course information bundles through it and expend the transmitted parcels.

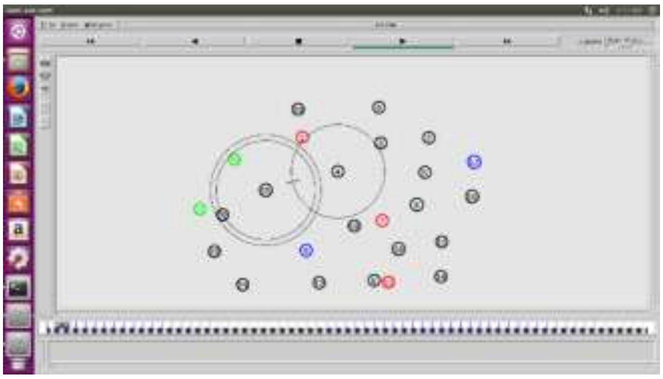

Fig 2: - Creating Black hole

Here, during the transmission of the packet from source to destination, the black hole node, which is 7, takes the entire packet and does not forward it to another node.

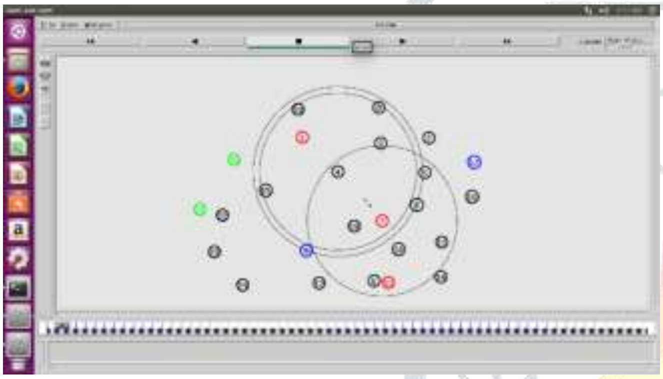

Fig 3: - node 7 takes the entire packet

Detecting and Preventing black hole Attack: We used our proposed technique to detect black hole attacks. According to our technique we detect nodes 1, 7 and 13 as black hole nodes.

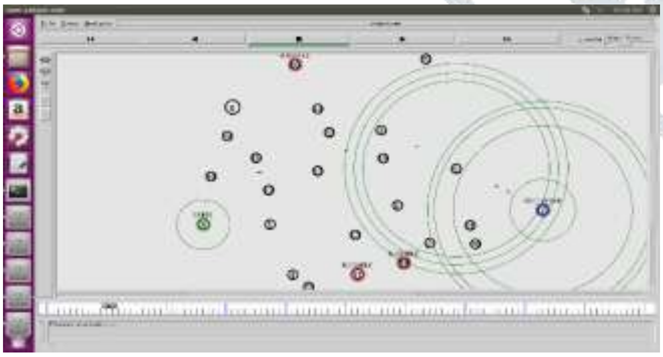

Fig 4: -Packet sends from Source to Destination

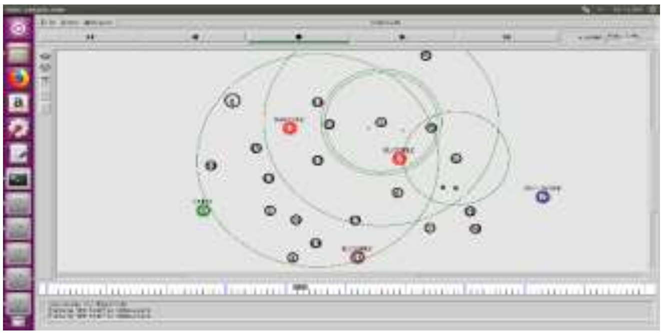

Fig 5(a): - Detecting & Preventing Black hole

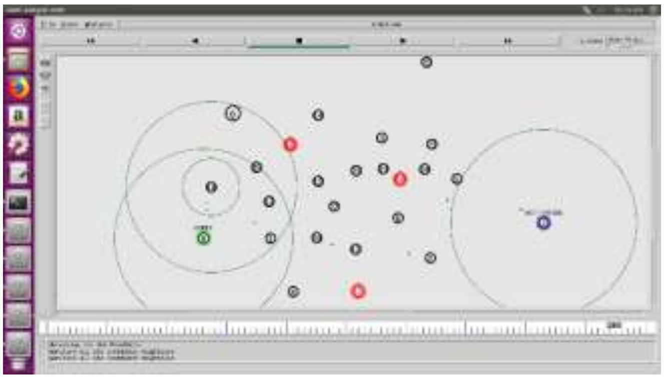

Fig 5(b): - Detecting & Preventing Black hole

VII. CONCLUSION

MANETs have been a territory of dynamic research in the course of recent years because of their possibly across the board application in military and regular citizen correspondence. In any case, MANETs are to a great degree powerless against assaults because of their powerfully evolving topology, nonappearance of regular security, open medium of correspondence. Versatile Ad-hoc Network is confronting numerous issues identified with the security. In our proposed framework, we have dissected the conduct and difficulties of security dangers in portable Ad-Hoc coordinates with dark gap identification method. In this paper, one kind of assault, the dark gap, which can be conveyed against the MANET is portrayed and an achievable answer for it in the AODV convention is proposed. A Black Hole assault is a sort of dissent of administration assault where a malevolent hub can draw in all parcels by dishonestly asserting a crisp course to the goal and afterward expend them without sending them to the goal.

VIII. FUTURE WORK

In our examination we utilize a few vindictive hubs so you can attempt with more pernicious hubs and assess the execution of MANET utilizing another steering convention. There is a need to do look into on other security assaults like jellyfish assault, dark opening assault, wormhole assault and so forth.

IX. ACKNOWLEDGMENT

I would first like to thank prof. Chandresh D. Parekh for his mentorship and guidance on my experiment. I would like to extend a special thanks to My family members for their affection, care and encouragement. Above all I am thankful to almighty God for everything.

X. REFERENCES

[1]. D. Mudzingwa and R. Agrawal, “A study of methodologies used in intrusion detection and prevention systems (IDPS)," IEEE, pp. 1-6, March 2012.

[2]. R. Akbani, T. Korkmaz, and G. V. S. Raju, “Mobile Ad hoc Network Security,” in Lecture Notes in Electrical Engineering, vol. 127. New York: Springer-Verlag, 2012, pp. 659–666.

[3]. Elhadi M. Shakshuki, Senior Member, IEEE, Nan Kang, and Tarek R. Sheltami, Member, IEEE “EAACK—A Secure Intrusion-Detection System for MANETs”, IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 60, NO. 3, MARCH 2013.

[4]. B. Sindhu1 M.E, Karpagam University, “A Survey on Intrusion Detection in Mobile Ad Hoc Networks Using Enhanced Adaptive Acknowledgment”, International Journal of Innovative Research in Computer and Communication Engineering, Vol.2, Special Issue 1, March 2014.

[5]. S.Rajeswari, Dr. A.Ramamurthy, K.T.V Subbarao, “An

Efficient Intrusion-Detection Mechanisms To Protect Manet From Attacks" , International Journal of Science Engineering and Advance Technology, IJSEAT, Vol 2, Issue 12, December – 2014.

[6]. Adnan Nadeem, Member, IEEE and Michael P. Howarth, "A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks", IEEE COMMUNICATIONS SURVEYS & TUTORIALS, ACCEPTED FOR PUBLICATION.

[7]. Ram Kishore Singh, Parma Nand, "Literature Review of Routing Attacks in MANET", international Conference on Computing, Communication and Automation (ICCCA2016).

[8]. Dr Sanjeev Yadav, Rachna Jain, Mohd Faisal, "Attacks in MANET", International Journal of Latest Trends in Engineering and Technology (IJLTET), ISSN: 2278-621X, Vol. 1 Issue 3 September 2012.

[9]. P. Narendra Reddy, CH. Vishnuvardhan, V. Ramesh, "ROUTING ATTACKS IN MOBILE AD HOC NETWORKS", IJCSMC, Vol. 2, Issue. 5, May 2013, pg.360 – 367.

[10]. I. Meenatchi , K. Palanivel, "Intrusion Detection System in MANETS: A Survey", International Journal of Recent Development in Engineering and Technology, ISSN 2347 – 6435, Volume 3, Issue 4, October 2014. José Helano Matos Nogueira The International Journal of FORENSIC COMPUTER SCIENCE IJoFCS (2006) 1, 28-32.

[11]. Latha Tamilselvan, Dr. V Sankaranarayanan, "Prevention of Blackhole Attack in MANET", The 2nd International Conference on WirelessBroadband and Ultra Wideband Communications (AusWireless 2007).

[12]. Ms.Chetana Khetmal1, Prof.Shailendra Kelkar2, Mr.Nilesh Bhosale3, " MANET: Black Hole Node Detection in AODV", international Journal of Computational Engineering Research||Vol, 03||Issue, *6*||

[13]. Farhin Shaikh, Chandresh Parekh, "A Review Paper on Intrusion Detection System in MANETs" International Journal of Scientific Research in Computer Science, Engineering and Information Technology | Volume 2 | Issue 6 | ISSN: 2456-3307