Journal of Advances and Scholarly Researches in Allied Education
Vol. 13, Issue No. 1, April-2017, ISSN 2230-7540

An Analysis upon Impact of Different Types of Attacks in Manet: Performance Evaluation

Anita Bhatia[1]* Dr. Kalpana[2]

[1]Research Scholar of OPJS University, Churu, Rajasthan

[2]Assosicate Professor, OPJS University, Churu, Rajasthan

Abstract – As of late, Mobile Ad-hoc Networks have gotten an enormous consideration in both industry and academia as they give dynamic networking services. Such networks are quickly deployable later on, so secure wireless environment will be required. In mobile ad hoc networks, because of temperamental wireless media, absence of settled framework and host mobility, giving secure communications is a major test. Since an impermanent gadget intermittently joins or leaves a network, the authentication and security innovation ought to be prepared for the vindictive gadgets utilized as a part of outsider attacks. Normally, symmetric and hilter kilter cryptographic methods are utilized for secure communications in wired and wireless networks yet they have their advantages and disadvantages.

MANET is a sort of Ad Hoc network with mobile, wireless nodes. In light of its uncommon characteristics like dynamic topology, bounce by-jump communications and simple and speedy setup, MANET confronted loads of challenges symbolically routing, security and clustering. The security challenges emerge because of MANET's self-configuration and self-upkeep capacities. In this investigation, we display an elaborate perspective of issues in MANET security. Based on MANET's uncommon characteristics, we characterize three security parameters for MANET. In addition we separated MANET security into two distinct aspects and examined everyone in subtle elements. An extensive investigation in security aspects of MANET and overcoming approaches is introduced. In addition, vanquishing approaches against attacks have been assessed in some important metrics. After examinations and assessments, future extents of work have been introduced.

----------X----------

INTRODUCTION

As mobile ad hoc networks (MANETs) are made immediately with mobile nodes that constantly change locations they are especially helpless to attack. A few attack mechanisms have been proposed and mostly comparing identification and counter measures. In any case, the lion's share of these methodologies have been dissected and assessed with incongruent objectives, changing setups and performance metrics. Simulation results are therefore not commensurate because of use particular parameter sets and execution contrasts. The target of our examination is to execute and assess the most unmistakable attacks utilizing a predictable and near system. The general effect of each attack is captured and completely examined based on a suitable arrangement of performance metrics. We characterize necessities for careful and steady catching of the impacts of all considered attack writes. A far reaching rundown of metrics is chosen as needs be and utilized for the investigation utilizing different blends of attack composes and parameter sets.

We look at conceivable strategies of attacking nodes to expand their effect while limiting their danger of discovery, and demonstrate the effect of the researched attacks on the network performance. Utilizing our results attackers can pick a setup with lowest recognition likelihood and MANET administrators can assess harm levels of a particular attack compose and decide adequate counter measures.

Performance metrics characterized in this investigation empower a steady examination of a range of attack composes with different parameters sets which can give further understanding into the communication and effect of attacking nodes on MANETs. Our assessment results demonstrate that the level of effect of attacks varies significantly depending on attack write and parameters utilized. The effect of specific kinds of attacks increments if a bigger number of attackers are available though specific attack writes (e.g. flooding and route interruption attacks) are most proficient when a solitary attacker is available.

A mobile ad hoc network (MANET) is a self-arranging network of mobile nodes. It does not have any settled framework like access points or base stations. It needs brought together administration and is connected by wireless links/links. Wireless ad hoc network can be develop where there is no help of wireless access or wired spine isn't possible. All network services of ad hoc network are arranged and made on the fly. Along these lines clearly with absence of infrastructural bolster and vulnerable wireless link attacks, security in ad hoc network ends up plainly characteristic shortcoming. Nodes inside nomadic environment with access to normal radio link can without much of a stretch partake to set up ad hoc foundation. Be that as it may, the secure communication among nodes requires the secure communication link to impart. Before building up secure communication, link the node ought to be sufficiently skilled to distinguish another node. Subsequently node needs to give his/her way of life and additionally related certifications to another node. However conveyed personality and qualifications should be confirmed and secured with the goal that authenticity and integrity of conveyed character and certifications can't be addressed by recipient node. Each node wants to make certain that conveyed character and certifications to beneficiary nodes are not traded off. In this way it is fundamental to give security design to secure ad hoc networking.

We found that many of the by and by existing attacks have some regular highlights and have been ordered into various attacks based on their minor contrasts. So therefore we are attempting to classify them into two broad classifications: DATA traffic attacks and CONTROL traffic attacks. This will help in future planning of security measures which will be capable in alleviating those broad classifications in one go.

SECURITY ATTACKS IN MOBILE AD HOC NETWORKS

Security implies ensuring the privacy (confidentiality), availability, integrity and non-repudiation. Security suggests the distinguishing proof of potential attacks from unauthorized access, utilize, modification or annihilation. A security attack is any activity that bargains the security of information in an unauthorized way. The attack may modify, discharge, or deny data. The attacks on the MANETs can be broadly grouped into two classifications: passive and active attacks. Both passive and active attacks can be made on any layer of the network protocol stack.

Passive Attacks: A passive attack endeavors to recover significant information by tuning in to traffic channel without legitimate approval, yet does not influence system resources and the ordinary working of the network. Passive attacks are difficult to distinguish on the grounds that they don't include any alteration of the data. Figure 1 demonstrates a schematic depiction of a passive attacker C, eavesdropping on the communication channel amongst An and B.

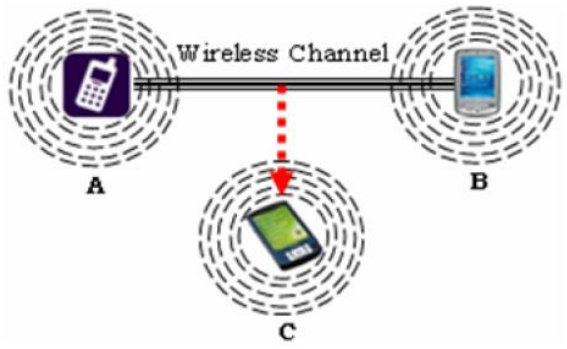

Figure 1: A passive attack.

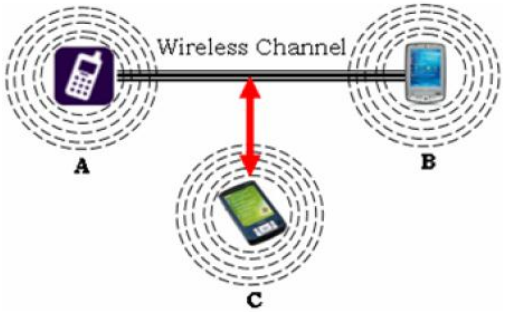

Figure 2: An active attack.

Active Attacks: An active attack endeavors to change or pulverize the system resources. It picks up an authentication and tries to influence or disturb the ordinary working of the network services by infusing or changing self-assertive packets of the data being exchanged in the network. An active attack includes information intrusion, modification, or fabrication. As appeared in Figure 2, an active attacker C can tune in, change, and infuse messages into the communication channel amongst An and B.

Active attacks can be either interior or outer . Outside attacks are done by mobile nodes that don't fit into the network. These attacks are propelled by adversaries who are not at first approved to partake in the network operations and access the resources without approval. Inner attacks are from agreeable mobile nodes that are a piece of the network.

Contrasted and outer attacks, interior attacks are more genuine and difficult to distinguish on the grounds that the attackers know significant and mystery information from traded off or seized nodes and have favored access rights to the network resources. Active attacks include activities, for example, impersonation (masquerading or mocking), modification, fabrication and replication. The active attacks are characterized into various kinds as appeared in Figure 3.

Jamming Attack - In this attack, the attacker fundamentally continues inspecting the wireless medium to discover the recurrence at which the collector node is accepting signals from the dispatcher. It, at that point, transmits signals on that specific recurrence so free gathering at the beneficiary is blocked without mistake .

Wormhole Attack - In this attack, a noxious node captures packets from one location in the network and "passages" these packets to alternate malevolent node at another location. The second noxious node is then anticipated that would replay the "burrowed" packets locally. The passage between two plotting attackers is considered as a wormhole. The wormhole can drop packets by shortcircuiting the customary flow of routing packets or it can precisely forward packets to maintain a strategic distance from location .

Black Hole Attack - This attack is a sort of denial of service where a noxious node pulls in all packets by erroneously guaranteeing (advertising) a briefest path to the destination node whose packets it wants to capture and, at that point, assimilate them without forwarding to the destination .

Sinkhole Attack - In this attack, the's adversary will likely pull in all the virtual traffic from a particular zone through a traded off node, making a representative sinkhole with the rival at the inside as nodes on or close to the path those packets follow have many chances to meddle with data .

Gray Hole Attack - A gray hole attack is a variety of the black hole attack, where the vindictive node isn't at first malevolent, it turns noxious sometime later. In this attack, an attacker drops all data packets however it lets control messages to route through it .

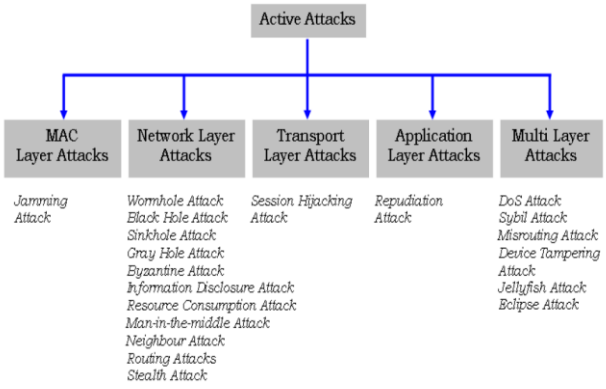

Figure 3: Classification of security attacks.

Byzantine Attack - In this attack, an arrangement of helpful intermediate nodes works in consolidated and all things considered performs attacks, for example, making routing circles, routing packets on most exceedingly bad paths, and selectively dropping packets.

Information Disclosure Attack - In this, a bargained node endeavors to uncover private or important information in regards to the network topology, geographic locations of nodes, or ideal routes to unauthorized nodes in the network .

Resource Consumption Attack - In this attack, a vindictive node purposefully tries to expend or abuse of the resources (battery power, bandwidth, and computational power) of other nodes' exist in the network by requesting inordinate route discovery (pointless route request control messages), exceptionally visit generation of reference point packets, or by forwarding superfluous packets (stale information) to that node .

Man-In-The-Middle Attack - In this attack, the attacker exists as a neighbor to any one node in the routing path and changes data that is being transmitted and infuses adjusted packet into network.

Neighbor Attack - The objective of neighbor attackers is to disturb multicast routes by making two nodes that are in reality out of communication range trust that they can discuss specifically with each other.

Routing Attacks - In this attack, attackers endeavor to change the routing information and data in the routing control packet. There are a few kinds of routing attacks mounted on the routing protocol which are intended for exasperating the operation of the network.

Stealth Attacks - Stealth attacks are ordered into two classes. The top of the line of attacks endeavors to perform traffic examination on separated traffic to and from casualty nodes. The below average segments the network and diminishes great put by disconnecting casualty nodes in a few ways. The strategies are alluded to as stealth attacks since they limit the cost of propelling the attacks.

Session Hijacking Attack – This attack is the real transport layer attack. Here, an adversary between two nodes takes control over a session. Once the session gets known between two nodes, the getting out of hand node conceals as one of the end nodes of the session and takes control over the session.

Repudiation Attack - Repudiation attack is the primary application layer level attack. Repudiation alludes to the dismissal or endeavored denial by a node associated with a communication of having contributed in a section or the whole communication. Non-repudiation is one of the key necessities for a security protocol in any

communication network and guarantees that a node can't later deny the data was sent by it.

Denial of Service Attack - In this attack, an adversary dependably endeavors to stay away from true blue and approved clients of network services from accessing those services, where genuine traffic can't achieve the objective nodes .

Sybil Attack - This attack is otherwise called masquerade or impersonation or ridiculing attack. In this attack, a single malicious node attempts to take out the personality of other nodes 'in the network by advertising false/fake routes. It then endeavors to send packets over network with personality of different nodes influencing the destination to trust that the packet is from original source .

Misrouting Attack-This attack is additionally known as manipulation of network traffic attack. This is an extremely straightforward way for a node to bother the protocol operation by reporting that it has better route than the existing one. In the misrouting attack, an on-real node redirects the routing message and exchanges data packet to the wrong target .

Gadget Tampering Attack-MANET no desaregenerally minimized, delicate, and hand-held in nature. They may be broken or lost or stolen effectively and abused by a rival.

Jellyfish Attack-A jellyfish attacker first necessities to barge in into the multicast forwarding group. It at that point interferes with data packets unreasonably for some time before forwarding them. This results high end-to-end delays and, in this way, degrades the constant applications performance .

Eclipse Attack-An example of trouble making called an eclipse attack, which consists of the gradual harming of good (uncompromised) nodes' routing tables with links to a conspiracy of adversarial nodes(compromised nodes) .

CLASSIFICATION OF ATTACKS

As already talked about, we have ordered the by and by existing attacks into two broad classifications: DATA traffic attacks and CONTROL traffic attacks. This grouping is based on their normal characteristics and attack objectives. For instance: Black-Hole attack drops packets without fail, while Gray-Hole attack additionally drops packets yet its activity is based on two conditions: time or sender node. Yet, from network point of view, the two attacks drop packets and Gray-Hole attack can be considered as a Black-Hole attack when it begins dropping packets. So they can be arranged under a solitary classification.

There are few attacks that have suggestions on the two DATA and CONTROL traffic, so they can't be grouped into these classes effortlessly. So those attacks are left for future discussions.

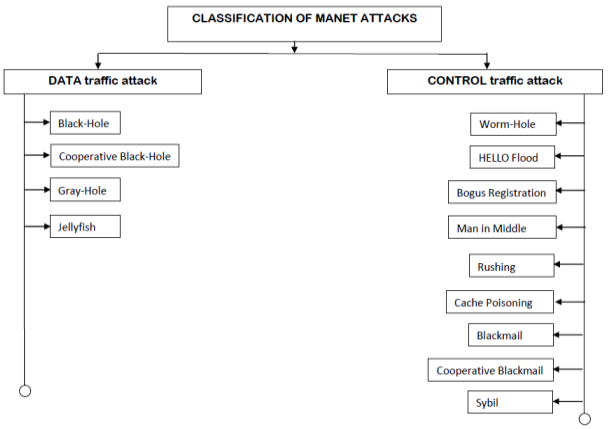

Figure 4: Classification of Mobile ADHOC Network (MANET) attacks.

DATA Traffic Attack -

DATA traffic attack deals either in nodes dropping data packets passing through them or in delaying of forwarding of the data packets. Some types of attacks choose victim packets for dropping while some of them drop all of them irrespective of sender nodes. This may highly degrade the quality of service and increases end to end delay. This also causes significant loss of important data. For e.g., a 100Mbps wireless link can behave as 1Mbps connection. Moreover, unless there is a redundant path around the erratic node, some of the nodes can be unreachable from each other altogether. 2.1.1 Black-Hole Attack In this attack, a malicious node acts like a Black hole, dropping all data packets passing through it as like matter and energy disappears from our universe in a black hole. If the attacking node is a connecting node of two connecting components of that network, then it effectively separates the network in to two disconnected components.

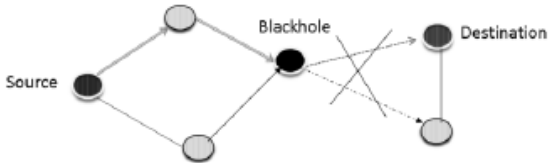

Figure 5: Black-Hole Attack.

Here the Black-Hole node separates the network into two sections. Hardly any strategies to relieve the issue:

(I) Collecting multiple RREP messages (from more than two nodes) and along these lines trusting multiple redundant paths to the destination node and after that buffering the packets until the point when a protected route is found.

(II) Maintaining a table in every node with past grouping number in expanding request. Every node before forwarding packets builds the succession number. The sender node broadcasts RREQ to its neighbors and once this RREQ achieves the destination, it answers with a RREP with last packet grouping number. In the event that the intermediate node finds that RREP contains a wrong grouping number, it comprehends that some place something turned out badly.

Agreeable Black-Hole Attack This attack is like Black-Hole attack, however more than one malevolent node tries to disturb the network at the same time. It is a standout amongst the most extreme DATA traffic attack and can absolutely disturb the operation of an Ad Hoc network. Generally the main arrangement progresses toward becoming finding rotating route to the destination, if at all exists. Location technique is like conventional Black-Hole attack. In addition another arrangement is securing routing and node discovery in MANET by any suitable protocol, for example, SAODV, SNRP, SND, SRDP and so forth. Since every node is already trusted, black hole node ought not show up in the network.

Gray-Hole attack has its own particular trademark conduct. It too drops DATA packets, however node's vindictive action is constrained to specific conditions or trigger. Two most normal kind of conduct:

(I) Node dependent attack – drops DATA packets predetermined towards a specific casualty node or originating from certain node (fig 6), while for different nodes it carries on typically by routing DATA packets to the destination nodes effectively.

(II) Time dependent attack – drops DATA packets based on some foreordained/trigger time while carrying on typically amid alternate examples. (fig. 7)

Recognizing this behaviorist attack is extremely troublesome unless there exists a system wide location algorithm, which deals with every one of the nodes performance in the network. Sometimes nodes can connect with each other and can advise noxious nodes presence to other friendly nodes. Approach is like Black-Hole attack where arrangement number criticism may distinguish some Gray-Hole attack. In the event that multiple paths exist amongst sender and destination at that point buffering packets with appropriate affirmation (for e.g. 2ACK) may identify active Gray-Hole attack in advance. Be that as it may, dormant or activated attack is hard to distinguish with this approach.

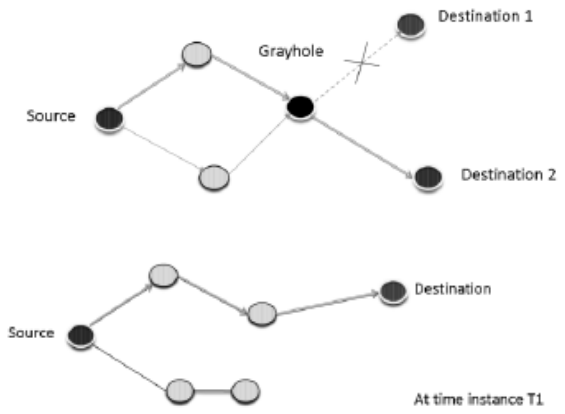

Figure 6: Gray-Hole – Node dependent attack

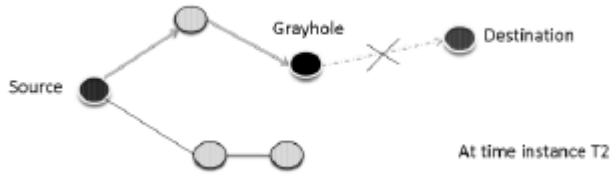

Figure 7: Gray-Hole – Time dependent attack.

Jellyfish Attack -

Jellyfish attack is fairly unique in relation to Black-Hole and Gray-Hole attack. Instead of aimlessly dropping the data packets, it delays them before at last conveying them. It might even scramble the request of packets in which they are gotten and sends it in irregular request. This disturbs the typical flow control system utilized by nodes for solid transmission. Jellyfish attack can bring about significant end to end delay and along these lines degrading QoS. Maybe a couple of the techniques utilized by attacker in this attack:

(I) One of the strategies is scrambling packet arrange before at last conveying them instead of got FIFO arrange. ACK based flow control instrument will generate copy ACK packets which will pointlessly expend valuable network bandwidth and battery life.

(II) Another strategy can be, performing selective Black-Hole attack by dropping all packets at each RTO. This will cause timeout in sender node at each RTO for that duration. On the off chance that nodes utilize traffic forming, default flow control instrument may be activated to the sender node as it is same as destination overpower

(III) The attacking node can store all the got packets in its cushion however sends them after some arbitrary delay keeping up the got packet arrange. Here likewise the flow

control instrument gets befuddled. Sometimes the source node may take a more extended route instead of the most clear briefest route.

Control Traffic Attack -

Mobile Ad-Hoc Network (MANET) is intrinsically powerless against attack because of its major characteristics, for example, open medium, distributed nodes, self-governance of nodes support in network (nodes can join and leave the network on its will), absence of unified specialist which can implement security on the network, distributed co-appointment and cooperation. The current routing protocols can not be utilized as a part of MANET because of these reasons.

Many of the routing protocols contrived for use in MANET have their individual trademark and standards. Two of the most broadly utilized routing protocols is Ad-Hoc On Demand Distance Vector routing protocol (AODV), which depends on singular node's cooperation in building up a legitimate routing table and Dynamic MANET On-Demand (DYMO) , which is a quick light weight routing protocol contrived for multi bounce networks. In any case, each of them is based on trust on nodes partaking in network. The initial phase in any effective attack requires the node to be a piece of that network. As there is no requirement in joining the network, malignant node can join and disturbs the network by hijacking the routing tables or bypassing legitimate routes. It can likewise listen in on the network if the node can set up itself as the most limited route to any destination by misusing the unsecure routing protocols. Accordingly it is of most extreme significance that the routing protocol ought to be as much secure as it can be.

Worm Hole Attack -

Worm hole, in cosmological term, connects two distant points in space through an easy route. Similarly in MANET likewise at least one attacking node can disturb routing by short-circuiting the network, in this way upsetting regular flow of packets. On the off chance that this link turns into the lowest cost path to the destination then these malignant nodes will dependably be picked while sending packets to that destination. The attacking node at that point can either screen the traffic or can even upset the flow (by means of one of the DATA traffic attack). Wormhole attack should be possible with single node additionally however for the most part at least two pernicious node connects by means of a wormhole-link. In figure 8, Node X and Y performing wormhole attack.

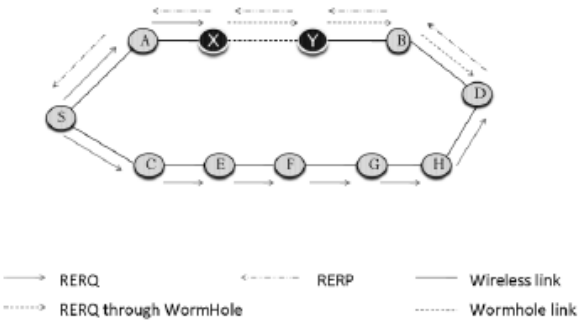

Figure 8: Worm-Hole attack.

There have been couple of proposals as of late to shield networks from worm-hole attack:

(I) Geographical chains and transient rope: A rope is added to every packet with a specific end goal to limit the distance the packets are allowed to movement. A rope is related with each jump. In this manner, every transmission of a packet requires another chain. A land rope is intended to restrain the distance between the transmitter and the collector of a packet. A transient chain gives an upper bound on the lifetime of a packet.

(II) Using directional antenna: Using directional antenna limits the bearing of signal engendering through air. This is one of the rough methods for restricting packet scattering.

Hello Flood Attack -

The attacker node floods the network with a high quality route with a powerful transmitter. In this way, every node can forward their packets towards this node trusting it to be a superior route to destination. Some can forward packets for those destinations which are out of the compass of the attacker node. A solitary high power transmitter can persuade that every one of the nodes are his neighbor. The attacker node require not generate a real traffic; it can simply play out a selective replay attack as its power overpowers different handsets.

Bogus Registration Attack -

A Bogus registration attack is an active attack in which an attacker camouflages itself as another node either by sending stolen reference point or producing such false signals to enlist himself with a node as a neighbor. Once enlisted, it can snoop transmitted packets or may upset the network by and large. In any case, this kind of attack is hard to accomplish as the attacker needs to personally know the masquerading nodes character and network topology. Encoding packets before sending and secure authentication in route discovery (SRDP, SND, SNRP, ARAN, and so on) will confine the

seriousness of attack to some degree as attacker node has no past knowledge of encryption strategy.

Man in Middle Attack -

In Man in Middle attack, the attacker node creeps into a legitimate route and tries to sniff packets flowing through it. To perform man in middle attack, the attacker first should be a piece of that route. It can do that by either incidentally disturbing the route by deregistering a node by sending pernicious disassociation reference point captured beforehand or enlisting itself in next route timeout occasion. One method for shielding packets flowing through MANET from prying eyes is scrambling every packet. In spite of the fact that key circulation turns into a security issue.

Rushing Attack -

In AODV or related protocol, every node before transmitting its data, first builds up a substantial route to destination. Sender node broadcasts a RREQ (route request) message in neighborhood and legitimate routes answers with RREP (route answer) with appropriate route information. A portion of the protocols utilize copy concealment component to constrain the route request and answer babble in the network. Rushing attack misuses this copy concealment system. Rushing attacker rapidly advances with a malevolent RREP for the benefit of some other node skirting any appropriate processing. Because of copy concealment, genuine substantial RREP message from legitimate node will be disposed of and subsequently the attacking node turns out to be a piece of the route. In rushing attack, attacker node sends packets to legitimate node after its own sifting is done, so from outside the network carries on typically as though nothing happened. Be that as it may, it may expand the delay in packet conveying to destination node.

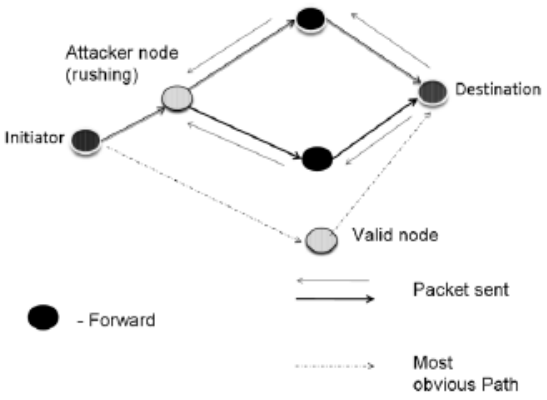

Figure 9: Rushing Attack

Maybe a couple of the protocols that may help in settling Rushing attack:

(I) SEDYMO : Secured Dynamic MANET On-Demand is like DYMO yet it directs intermediate node must add routing information while broadcasting the routing messages and no intermediate node ought to erase any routing information from past sender while broadcasting. It additionally incorporates hash fastens and digital signature to ensure the character.

(II) SRDP : Secure Route Discovery Protocol is security upgraded Dynamic Source routing (DSR) protocol.

(III) SND : Secure Neighbor Detection is another technique for checking each neighbor's personality inside a most extreme transmission range.

Store Poisoning Attack -

By and large in AODV, every node keeps few of its latest transmission routes until timeout happens for every passage. So each route waits for quite a while in node's memory. In the event that some malevolent node plays out a routing attack then they will remain in node's route table until timeout happens or a superior route is found. An attacker node can advertise a zero metric to the majority of its destinations. Such route won't be overwritten unless timeout happens. It can even advertise itself as a route to a distant node which is out of its span. When it turns into a piece of the route, the attacker node can play out its vindictive movement. Impact of Cache harming can be restricted by either adding limit chains or by token authentication. Additionally every node can keep up its friend-enemy list based on authentic measurements of neighboring nodes performance.

Blackmailing and Co-agent Blackmailing Attack-

In a blackmailing attack or all the more successfully co-agent blackmailing attack, attacker nodes denounce a pure node as hurtful node. This attack should successfully be possible on those distributed protocols that set up a decent and bad node list based on audit of taking an interest nodes in MANET. Maybe a couple of the protocols tries to influence them more to secure by utilizing dominant part voting rule, yet at the same time if adequate no. of attacker nodes turn out to be a piece of the MANET it can sidestep that security moreover.

Another nonexclusive strategy for this attack will be, sending invalid RREP messages with advertising a superfluously high cost to specific nodes.

Sybil Attack-

Sybil attack manifests itself by faking multiple characters by pretending to comprise of multiple nodes in the network. So one single node can expect the role of multiple nodes and can screen or hamper multiple nodes at a time. On the off chance that Sybil attack is performed over a blackmailing attack, at that point level of interruption can be very high. Accomplishment in Sybil attack depends on how the characters are generated in the system.

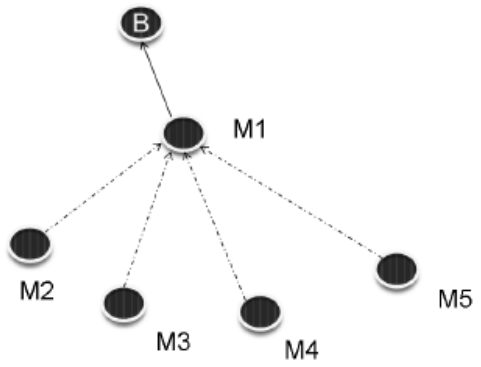

Figure 10: Sybil Attack

In figure 10, node M1 assumes identities of M2, M3, M4, and M5. So, to node B, M1 is equivalent to those nodes.

One way of mitigating this attack is maintaining a chain of trust, so single identity is generated by a hierarchical structure which may be hard to fake.

CONCLUSION

In this investigation we actualized and assessed the most noticeable attacks in a steady manner to give a compact correlation of attack writes and parameters. We characterized performance metrics that allow the capture and examination of effect levels for each attack compose on MANET performance. An exploration of the impacts and harm levels caused by a few attack writes and parameter sets has additionally been introduced.

Our assessment results demonstrate that the level of effect for each attack compose contrasts significantly depending upon parameters utilized. The effect of specific attacks increments impressively with an expanding number of attacking nodes in a few of the situations, though other attack affect levels remain relatively constant with fluctuating number of attackers.

These results suggest that an attacker could pick an attack strategy from various options with comparative general effect which limits location chance. This likewise recommends MANET administrators can utilize the results to gauge harm caused by different attacks to decide adequate counter measures.

Performance metrics laid out in this examination give a premise to predictable correlation of different attack writes and parameters and consequently a more profound understanding into the association and the effect of attacks in MANETs. The impact of changing simulation setups (e.g. as to territory and node mobility) however ought to be additionally researched in future work. Utilizing this structure future research on attacks in MANETs can concentrate on the most deceitful attacks and explore and look at in more detail their particular properties.

REFERENCES

Books –

Dimitris Glynos, Panayiotis Kotzanikolaou, Christos Douligeris (2008). "Preventing Im-personation Attacks in MANET with Multi-factor Authentication", IEEE transactions published at Department of Informatics, University of Piraeus, Greece.

Haining Wang, Danlu Zhang, and Kang G. Shin (2002). Detecting SYN Flooding Attacks, IEEE INFOCOM', New York City.

Raja, M.L. and Baboo, C.D.S.S. (2014). An Overview of MANET: Applications, Attacks and Challenges.

Yanchao Zhang, Wei Liu and Wenjing Lou (2009). *Anonymous Communications in Mobile Ad Hoc Network**s***.

Research Papers –

C. Karlof and D. Wagner (2002). "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Elsevier's Ad Hoc Networks J., Special ssuel on Sensor Network Applications Protocols, vol. 1, no. 2–3, pp. 293–315.

Mengbo Hou and Qiuliang Xu (2014). "*Key Replicating Attack on Certificateless Authenticated Key Agreement Protocol"*, Asia-Pacific Conference on Information Processing, pp. 47–50.

Mohd Izuan Mohd Saad and Zuriati Ahmad Zukarnain (2009). "Performance Analysis of Random-Based Mobility Models in MANET Routing Protocol", European Journal of Scientific Research, vol. 32, no.4, pp. 444-454.

Ping Yi, Zhoulin Dai, Shiyong Zhang, Yiping Zhong (2011). —A New Routing Attack in Mobile Ad Hoc Networks International Journal of Information Technology Vol. 11 No. 2, pages 83 – 94.

R. Maheshwari, J. Gao, and S. R. Das (2007). "Detecting Wormhole Attacks in Wireless Networks Using Connectivity Information," Proc. IEEE INFOCOM '07.

Sunil Taneja and Ashwani Kush (2010). "A survey of Routing Protocols in Mobile Ad Hoc Networks" , International Journal of Innovation, Management and Technology, Vol. 1, No. 3, ISSN: 2010-0248

Umang Singh (2011). "Secure Routing Protocols in Mobile Adhoc Network-A Survey and Taxonomy" International Journal of Reviews in Computing. Vol. 7

Y. Zhang and Y. Fang (2005). "ARSA: An attack-resilient security architecture for multi-hop wireless mesh networks," IEEE J. Sel. Areas Commun., vol. 24, no. 10, pp. 1916–1928.

Internet –

Juan-Carlos Ruiz, Jesús Friginal, David de-Andrés, Pedro Gil : Black Hole Attack Injection in Ad hoc Networks www.ece.cmu.edu/~koopman/dsn08/fastabs/dsn08fastabs_ruiz.pdf

Mohammad Al-Shurman and Seong-Moo Yoo : Black Hole Attack in Mobile Ad Hoc Networks http://engsci.aau.dk/kurser/ETC/Wms2/Papers/Ad-hocSec/Sub/al shurman.pdf

---

Corresponding Author

Anita Bhatia*

Research Scholar of OPJS University, Churu, Rajasthan

E-Mail –