Journal of Advanced Computing and Communication Technologies *(ISSN:* **2347 - 2804***)*
Volume No.2 Issue No. 3, June 2014

PACKET DROPPING ATTACKS IN MANET: A SURVEY

By

[1]Kshitij Bhargava, [2]Dinesh Goyal
[1]M.Tech Scholar, Suresh Gyan Vihar University, Jaipur,INDIA
[2]Associate Professor, Suresh Gyan Vihar University, Jaipur, INDIA
[1] bhargavakshitij@gmail.com, [2]dinesh8dg@gmail.com

ABSTRACT

Due to the numerous applications areas of mobile ad-hoc networks (MANETs) such as military and war communications, disaster recovery, vehicular ad hoc networks (VANETs) etc. These wireless networks became targets of different types of attacks caused by various methods used by the attackers. Furthermore, the multi-hop communication in MANETs requires intermediate nodes to perform data communication between a source- destination pair. This provides a chance to the attackers to either steel the identity of the legitimate intermediate node or directly become part of the discovered route that will be used for data communication. In this way, MANETs are very vulnerable to various kinds of attacks. Also, a large number of applications over MANETs are increasing exponentially during recent years because of the advancements in the hardware design of hand-held devices and deployment mechanisms of wireless networks. This growing popularity of MANETs is one of the reasons due to which the number of attacks is increasing in these networks. At present many researchers working on the field of MANETs are working towards the analysis of various attacks that are injected in MANETs and also try to develop solution to either detect or prevent these attacks. In this paper, we present a detailed survey on various types of packet dropping attacks that are proposed in the recent years by various researchers working on the areas of attacks over MANETs with their detection methods (if given and available in the literature).

Keywords

Packet Dropping Attacks, Denial of Service Attacks, Mobile ad-hoc networks, MANETs

1. INTRODUCTION

Mobile ad-hoc networks (MANETs) are collection of mobile nodes that can communicate with each other using single or multiple hop fashion. Nodes that are with each other's transmission range communicate using single hop while intermediate nodes are used for multi-hop communication when source destination nodes are outside from each other's transmission range. These multi-hop communications are main target for malicious nodes for performing their various forms of attacks to degrade the performance of the network in terms of throughput and performance. The existing routing protocols used for routing in MANETs are not equipped with any mechanisms to handle any form of attack performed by a malicious node. The current routing protocols assume that each intermediate node is trustworthy and will deliver the data packets towards the destination node if selected as an intermediate node.

This form of blind trust is required for proper functionality of such networks due to their infrastructure less and un-centralized nature of communication. Therefore, its comparatively easy for attacker nodes to target such networks as compared to other types of data communication networks. This lack of any form of security measure to stop or avoid or to detect such malicious nodes makes these networks less suitable for a large array of important applications such as military operations or disaster management situations where they are required most. Without significant network layer or MAC layer security mechanisms enclosed, the current MANET routing solutions are much open to various forms of malicious attacks that can significantly degrade or freeze the whole network performance. In this paper, we will present an extensive study for various attacks that exists in MANETs by exploiting the vulnerabilities which already exists in its current routing mechanisms. We study how the existing routing protocols route discovery mechanism and their routing functions used for forwarding a packet or message can easily jeopardize the whole network performance.

In the light of the above discussed problems in the MANET, it is important to provision security measures to secure these networks - wired or wireless for its normal functionality. MANETs are more vulnerable to security threats than Wireline networks because of their inherent characteristics such as wireless communication medium, multi-hop routing and un-centralized control. Each node in MANET is independent i.e., they are free to join, move and leave the network anytime they want, this makes it susceptible to various attacks - both from inside or outside the network. The attacks can be launched by nodes within radio range or through compromised nodes. The compromised nodes exploit the flaws and inconsistencies present in routing protocol to destroy normal routing operation of the network. A compromised node may advertise nonexistent or fake links or flood honest nodes with routing traffic causing.

PACKET DROPPING ATTACKS IN MANETs

The following attacks are given in the literature:

Flooding Attack

In this attack proposed by **Ping Yi et al. [24]**, when used against an on-demand ad hoc network routing protocol, a malicious node generates a large number of fake route requests (RREQ) addressed to a destination that does not exist in the network. Since these route requests will never receive a reply, they will flood the entire network and congest the links. This results in the exhaustion of network resources, like bandwidth consumption, as well as consumption of a node's resources, like computational and battery power. Hence this attack is also known as sleep deprivation or resource consumption attack. This attack deteriorates the performance of the network by disrupting the routing operation. It eventually leads to denial of service.

Solutions Proposed: One mechanism proposed by **Ping Yi [19]** to prevent the flooding attack is known as the *neighbor suppression*. In this every node monitors and calculates the rate of its neighbors' RREQ. If this rate exceeds the predefined threshold, the ID of this neighbor is recorded in the node's blacklist. Consequently all the requests coming from the nodes listed in the blacklist table are dropped.

But this method fails against flooding attack in which the flooding rate is below the threshold. Hence to overcome this limitation another approach is used, in which statistical analysis is used to detect malicious RREQ floods. And unlike the previous mechanism here the threshold is not predefined and static. This technique determines the threshold based on a statistical analysis and therefore considerably reduces the attack from malicious nodes having varying flooding rates.

Black hole Attack

Mishra et al. [1] proposed an attack called black hole attack. In a black hole attack, after hearing the route request packet in the network the attacker node claims to have an extremely short route to the requested destination. The attacker does so by sending a fabricated RREP to the source node. In this RREP, the destination sequence number is set to be equal to or greater than the one contained in RREQ. This gives the source node the false impression that the malicious node has the freshest route to the destination. Hence the source node chooses the route passing through the attacker to send the data packets. Now since most of the network traffic passes through the malicious node, it can either drop the packets or manipulate the traffic in any way it wants.

Solutions proposed: **Dhurendhar et al [2]** proposed approach to overcome this attack is introduction of additional control packets such as CREQ and CREP i.e. route confirmation request and route confirmation reply respectively. In this method, the intermediate node along with sending RREPs to the source node also sends CREQs to its next-hop node towards the destination node. If this neighbor has a route it sends CREP to the source node. When the source node receives the CREP, it compares the path in RREP and CREP. If the paths match then the route is confirmed to be valid.

But this approach has a limitation. It doesn't work if two malicious nodes are placed consecutively. The adjoining malicious node sends CREPs that support the incorrect path. Hence to solve this issue another mechanism was proposed in which the source node is required to wait until RREP packets are received from multiple nodes. After that the source node checks that if there's a shared hop or not in these RREPs. If there is, then the route is considered to be correct else the route is invalid. However this method leads to time delay.

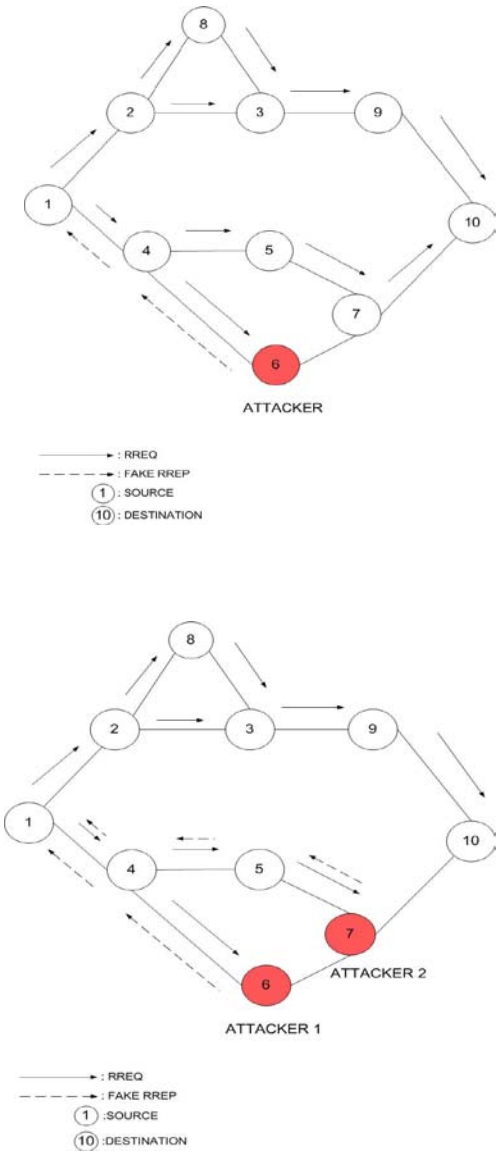

Figure 1: Black hole attack in MANET

In a much better solution, statistical based anomaly detection is used to detect the black hole attack [2]. The difference between the destination sequence numbers of the received RREPs is analyzed in this method. If the difference is considerably huge then the route is considered wrong. However this approach is prone to false positives.

Wormhole attack

Ahuja et al. [5] has proposed an attack which is also known as the tunneling attack, this attack is possible even if the attacker has not compromised any other legitimate nodes and even if all communication provides authenticity and confidentiality. Hence it is one of the most severe and sophisticated attacks in mobile ad hoc networks. In this attack, a pair of malicious nodes is connected through a high speed network, also known as the tunnel. Here, when the attacker receives a RREQ, it forwards it to its colluding partner through the tunnel. The malicious node on the other side of the tunnel, after receiving this RREQ, replays it to its neighboring nodes. This route request would be the first to reach the destination node since it has travelled through a faster medium than the links between legitimate nodes. Therefore the colluding nodes would most probably be included in the route, which would give them the freedom to misuse or discard packets.

Solutions proposed: In order to combat this attack, two types of leashes are used, temporal leashes and geographical leashes. In temporal leash method, the expiration time, t, is calculated in order to specify the maximum distance, L, which can be travelled by a packet. The malicious node cannot alter the expiration time since TIK is used to authenticate the expiration time in this method. This approach requires all nodes to have tightly synchronized a clock which serves as a drawback. On the other hand, in case of geographical leashes the nodes have loosely synchronized clocks. In this approach every node should know its position and while sending a packet it should also include its current position and sending time. Now the receiver can compute its distance from the sender and as a result can inspect neighbor relations.
Another approach is the use of a statistical analysis of multipath (SAM). Here the relative frequency of each link that appears in routes obtained from one route discovery is calculated. The link having the highest relative frequency is considered the wormhole link.

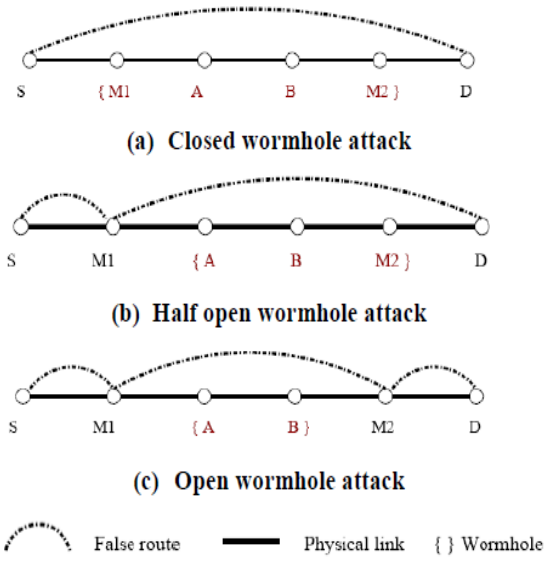

Figure 2: Classification of wormhole attacks in MANETs [30]

Selective Forwarding Attack

This attack is also known as the gray hole attack proposed by **Khattak[3]**. This attack is a refined version of black hole attack. Unlike black hole attack, here the malicious node drops only selected packets and forwards other packets, hence making the detection of malicious node difficult. This attack can be conducted in various ways. The attacker can either select a certain source or destination address and can refuse to forward or drop all the packets containing the respective source or destination addresses, or the attacker can randomly select the packets to be dropped. The former causes denial of service attack for a particular node. Another form of selective forwarding attack is to delay packets passing through the attacker and therefore creating confused routing information between the nodes.

Selfish Node Attack

In this attack, the node stops using its resources such as bandwidth etc, it stops forwarding or relaying packets. It does so without the network knowing. It does not participate in any of the network operations but uses it for its selfish purposes like saving its own resources like power. This results in highly decreased performance of the network

Link Spoofing Attack

In this attack, a malicious node presents false information of having a link with non-neighbors. In OLSR, for example, the attacker can convince the source to include it in its MPR set by presenting false information of having a link to its two-hop neighbors. After the malicious node is chosen to be its MPR, it gets the authority to alter the traffic as desired. It can as a result drop the packets or withhold them in order to degrade the performance of the network immensely.

Solution proposed: The first approach uses cryptography with a GPS and a time stamp to detect the attack and is known as location information-based detection method. It requires the node to be equipped with a GPS device which is the main limitation of this solution.
Another solution requires addition of two-hop information to a HELLO message, which every node being aware of complete topology up to three hops. This would result in every node being able to detect inconsistency in the event of an attack.

Sybil attack

Here the single attacker node behaves as if it were a group of a number of nodes. It appears to other nodes as a number of different nodes but it is actually a single malicious node. By doing so, it can prevent other nodes from using those addresses. A Sybil attack can be performed in various forms. In Sybil attack, a Sybil node can obtain the identity in two ways either by stealing other node's identity i.e. impersonation or by fabricating false identities. The Sybil node can communicate both directly and indirectly with the legitimate nodes. Also the attacker can have his Sybil identities all participate in the network at once i.e. simultaneously or they can participate in fractions i.e. non-simultaneously. As a result in routing, the seemingly disjoint paths could in fact go through a single malicious node presenting several Sybil identities. These identities can manipulate the traffic by disrupting routing operation.

Blackmail Attack

In this attack a legitimate node is misrepresented as a malicious node by the attacker node. Here the malicious node makes an entry of a legitimate node in its blacklist table giving false appearance of being malicious to the legitimate node. This attack occurs against protocols that uses attack detection mechanisms like watchdog and path rater. The malicious node exploits the vulnerabilities of these mechanisms to blackmail a legitimate node. The attacker node thus provokes other legitimate nodes to put this target legitimate node as an attacker in their blacklist table. This results in a good node being considered as a bad node by the network.

Location Disclosure Attack

In location disclosure attack, the attacker with the help of traffic analysis techniques or simpler probing and monitoring approaches can get access to highly confidential and important information such as location of nodes, structure of the entire network etc. Here the traffic is analyzed in order to know the traffic patterns and track changes, also the identities of the communicating nodes is collected, after which further attack is planned and launched. This attack is aimed to hamper with the privacy aspect of the network and is lethal for security sensitive scenarios.

Detour Attack

Also known as the gratuitous detour attack, this attack is specific to source routing protocols. This attack detours traffic through congested or energy-depleted routes by modifying the route request metrics in such a way that it appears more costly than the route that the attacker aims to detour traffic to. The traffic can be detoured in many ways such as increasing the hop count or delaying rebroadcasting route requests. Also the malicious node during route discovery phase adds a number of virtual nodes to the route. As a result the traffic is deflected to other routes which might appear shorter and less costly. These routes might have other malicious nodes which might launch other attacks. Due to this detour, the energy of the malicious node is saved highly since it doesn't have to forward packet to the destination itself.

Attack	Attack Type	Effect on data communication	Detection Mechanisms
Black hole Attack	Non-co-operative	Degrade packet delivery ratio	Watchdog
Wormhole Attack	Co-operative (Needs at least two attackers)	Degrade packet delivery ratio	ACK-based schemes
Jellyfish Attack	Co-operative or Non-co-operative	Degrade End-to-end delay and packet delivery ratio	Reputation-based schemes
Rushing or Flooding Attack	Non-co-operative	Increase routing overhead and network contention and congestion	Incentive-based schemes
Sybil Attack	Non-co-operative	Degrade packet delivery ratio and provide false network topology information	Lightweight Sybil Attack Detection
Node-misbehavior Attack	Co-operative or Non-co-operative	Provide false network topology information and increase jitter	CONFIDANT
Gray hole Attack	Non-co-operative	Degrade packet delivery ratio	Ex-Watchdog

Figure 3: Comparison between Different Packet Dropping Attacks

2. CONCLUSION AND FUTURE WORK

In this paper, we have presented an extensive survey on various forms of packet dropping attacks performed on mobile ad hoc networks. We have surveyed different dropping attacks performed on various MANET routing protocols and summarized their working methodology and their impact on communication process. We have also analyzed the prevention techniques for the reviewed attacks presented in literature to identify their effectiveness in detection and countermeasure process.

In the future work, we will try to find effective solutions to detect the malicious nodes and will remove them from network for further communication. The effectiveness of the proposed solution will be measured for both the attacks and its detection rate should be kept as much as high that we can. We also work to provide a single defense mechanism for both the attacks with the lowest routing overhead possible.

REFERENCES

[1]. Ankur mishra, Ranjeet Jaiswal, Sanjay Sharma "A Novel Approach for Detecting and Eliminating Cooperative Black Hole Attack using Advanced DRI Table in Ad hoc Network" 2013 3rd IEEE International Advance Computing Conference

[2]. Sanjay K. Dhurandher, Isaac Woungang, Raveena Mathur and Prashant Khurana "A Modified AODV against single and collaborative Black Hole attacks in MANETs" 2013 27th International Conference on Advanced Information Networking and Applications Workshops

[3]. Hizbullah Khattak, Nizamuddin, Fahad Khurshid, Noor ul Amin "Preventing Black and Gray Hole Attacks in AODV using Optimal Path Routing and Hash" 978-1-4799-0615-4/13/$31.00 ©2013 IEEE

[4]. P. R. Jasmine Jeni A. V imala Juliet R.Parthasarath/ A.Messiah Bose "Performance Analysis of DOA and AODV Routing Protocols with BlackHole Attack in MANET" 2013 International Conference on Smart Structures & Systems (JCSSS-20 13), March 28 - 29, 2013, Chennai, INDIA

[5]. Ravinder Ahuja Alisha Banga Ahuja Pawan Ahuja "Performance Evaluation and Comparison of AODV and DSR Routing Protocols in MANETs Under Wormhole Attack" Proceedings of the 2013 IEEE Second International Conference on Image Information Processing (ICIIP-2013)

[6]. Seryvuth Tan Keecheon Kim "Secure Route Discovery for Preventing Black Hole Attacks on AODV-based MANETs

[7]. Jyoti Rani, Naresh Kumar ":Improving AOMDV Protocol for Black Hole Detection in Mobile Ad hoc Network" 2013 International Conference on Control, Computing, Communication and Materials (ICCCCM).

[8]. Thongchai Chuachan Somnuk Puangpronpitag "A Novel Challenge & Response Scheme against Selective Forwarding Attacks in MANETs" 978-1-4673-5990-0/13/$31.00 ©2013 IEEE.

Issa Khalil, Sameer Bataineh, Liana Qubajah and Abdallah Khreishah "Distributed Secure Routing Protocol for Mobile Ad-Hoc Networks" 2013 5th International Conference on Computer Science and Information Technology (CSIT)

[9]. Sunil J. Soni Suketu D. Nayak " Distributed Secure Routing Protocol for Mobile Ad-Hoc Networks" 2013 International Conference on Intelligent Systems and Signal Processing (ISSP)