ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

A Survey of Network Layer Attacks in MANET Using Sequence Diagram

Medini Desai, Prof. S. A. Nagtilak

Department of Information Technology, Smt. Kashibai Navale College of Engineering, Pune, India

Department of Information Technology, Smt. Kashibai Navale College of Engineering, Pune, India

ABSTRACT: MANET is a collection of the autonomous node. Mobility, dynamic topology, and self-organization of nodes are the features of MANET. Due to these intrinsic features, MANET is more vulnerable to security attack than the traditional wired network.
Security Prevention implemented for the traditional network is not suitable for MANET. To develop more secure and effective intrusion detection system, one must aware of possible security attack.
Due to dynamic topology and multi-hop routing technique, the network layer of MANET prone to many attacks. In this paper, well-known network layer security attacks are modeled using a sequential diagram approach of Unified Modeling Language (UML).

KEYWORDS: MANET, UML, Sequence Diagram, Network Layer Attack.

I. INTRODUCTION

MANET is the collection of autonomous nodes which are mobile innature and communicate with each other using multi- hop technique. The main purpose of MANET is to provide communication in some situations where the services offered by both wired networks and WLAN are unavailable. MANETs are mainly useful for military and other applications such as emergency rescues. Security in MANET is more complex mainly due to its intrinsic features like mobile nodes, limited physical security, changing topology, scalability and lack of centralized management. A MANET is more prone to many different security attacks at all layers of communication, and these attacks can launch a lot of in consistencies in the network. To develop good intrusion detection and prevention system, it is essential to understand the behavior of the attacks [7]. MANET based on open network architecture it allows a peer to peer connectivity between nodes [6]. Network layer plays a central part in the operation of MANET where it is responsible for determining and maintaining network routes, delivery of packet from source to destination. Coo perative nature of network layer protocols makes network layer vulnerable to many different attacks such as Blackhole, wormhole, sleep attacks, sibyl attack, etc. These attacks introduce significant delays in the network, congestion and performance degradation.

Understanding the behavior of network layer attacks is important to develop secure mechanisms for MANET. The aim of this paper is to understand and model the behavior of network layer attacks using UML sequence diagram.

II. RELATED WORK

Classification of Attacks in MANETS

Mobile Ad hoc networks are vulnerable to various attacks not only from outside but also from within the network itself. Ad hoc network are mainly subjected to two different levels of attacks [12]. The first level of attack occurs on the basic mechanisms of the ad hoc network such as routing. Whereas the second level of attacks tries to damage the security mechanisms employed in the network. The attacks in MANETs are divided into two major types [9].

- **Internal Attacks**

Internal attacks are directly leads to the attacks on nodes presents in network and links interface between them. This type of attacks may broadcast wrong type of routing information to other nodes. Internal attacks are sometimes more difficult to handle as compare to external attacks, because internal attacks occurs due more trusted nodes. The wrong

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

routing information generated by compromised nodes or malicious nodes are difficult to identify. This can be due to the compromised nodes are able to generate the valid signature using their private keys.

- **External Attacks**

These types of attacks try to cause congestion in the network, denial of services (DoS), and advertising wrong routing information etc. External attacks prevent the network from normal communication and producing additional overhead to the network. External attacks can classify into two categories [10]:

- **Passive Attacks**

MANETs are more susceptible to passive attacks. A passive attack does not alter the data transmitted within the network. But it includes the unauthorized "listening" to the network traffic or accumulates data from it. Passive attacker does not disrupt the operation of a routing protocol but attempts to discover the important information from routed traffic. Detection of such type of attacks is difficult since the operation of network itself doesn't get affected. In order to overcome this type of attacks powerful encryption algorithms are used to encrypt the data being transmitted.

- **Active Attacks**

Active attacks are very severe attacks on the network that prevent message flow between the nodes. However active attacks can be internal or external. Active external attacks can be carried out by outside sources that do not belong to the network. Internal attacks are from malicious nodes which are part of the network, internal attacks are more severe and hard to detect than external attacks. These attacks generate unauthorized access to network that helps the attacker to make changes such as modification of packets, DoS, congestion etc. The active attacks are generally launched by compromised nodes or malicious nodes. Malicious nodes change the routing information by advertising itself as having shortest path to the destination.

ACTIVE ATTACKS ARE CLASSIFIED INTO FOUR GROUPS:

i. **Dropping Attacks***:* Compromised nodes or selfish nodes can drop all packets that are not destined for them. Dropping attacks can prevent end-to-end communications between nodes, if the dropping node is at a critical point. Most of routing protocol has no mechanism to detect whether data packets have been forwarded or not.

ii. **Modification Attacks***:* Sinkhole attacks are the example of modification attacks. These attacks modify packets and disrupt the overall communication between network nodes. In sinkhole attack, the compromised node advertises itself in such a way that it has shortest path to the destination. Malicious node than capture important routing information and uses it for further attacks such as dropping and selective forwarding attacks.

iii. **Fabrication Attacks***:* In fabrication attack, the attacker send fake message to the neighbouring nodes without receiving any related message. The attacker can also sends fake route reply message in response to related legitimate route request messages [8].

iv. **Timing Attacks***:* In this type of attacks, attackers attract other nodes by advertising itself as a node closer to the actual node. Rushing attacks and hello flood attacks uses this technique [11].

III. ANALYSIS OF NETWORK LAYER ATTACK

A. *BLACK HOLE ATTACK*

Blackhole Attack comes under a Denial of Service attack (Dos) which can perform by single compromised node or set of compromised nodes. Blackhole attack abuses the nature of reactive routing protocol, and it works in two phases in the first phase Compromised node advertises itself as having the short and fresh route to the destination and drops the receiving packets without forwarding them further. The detailed procedure is as follows below in Fig.1

1) An attacker compromises a malicious node 3 and initiates for Blackholeattack
2) Source node1 detects an event to establish a route to destination node5.
3) Source node1 broadcast route request.
4) Legitimate node 2 receives and broadcast the same request.
   (Source node1→ legitimate node2→ legitimate node4→ destination node5)
5) Malicious node directly replies to source node with a high destination sequence number.
6) Source node select route via malicious node.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

7) Source node sends data packet. (Sourcenode1→ Maliciousnode2)
8) Malicious node2 refuses to transfer data packet.(Source node1→ malicious node2----DROP)

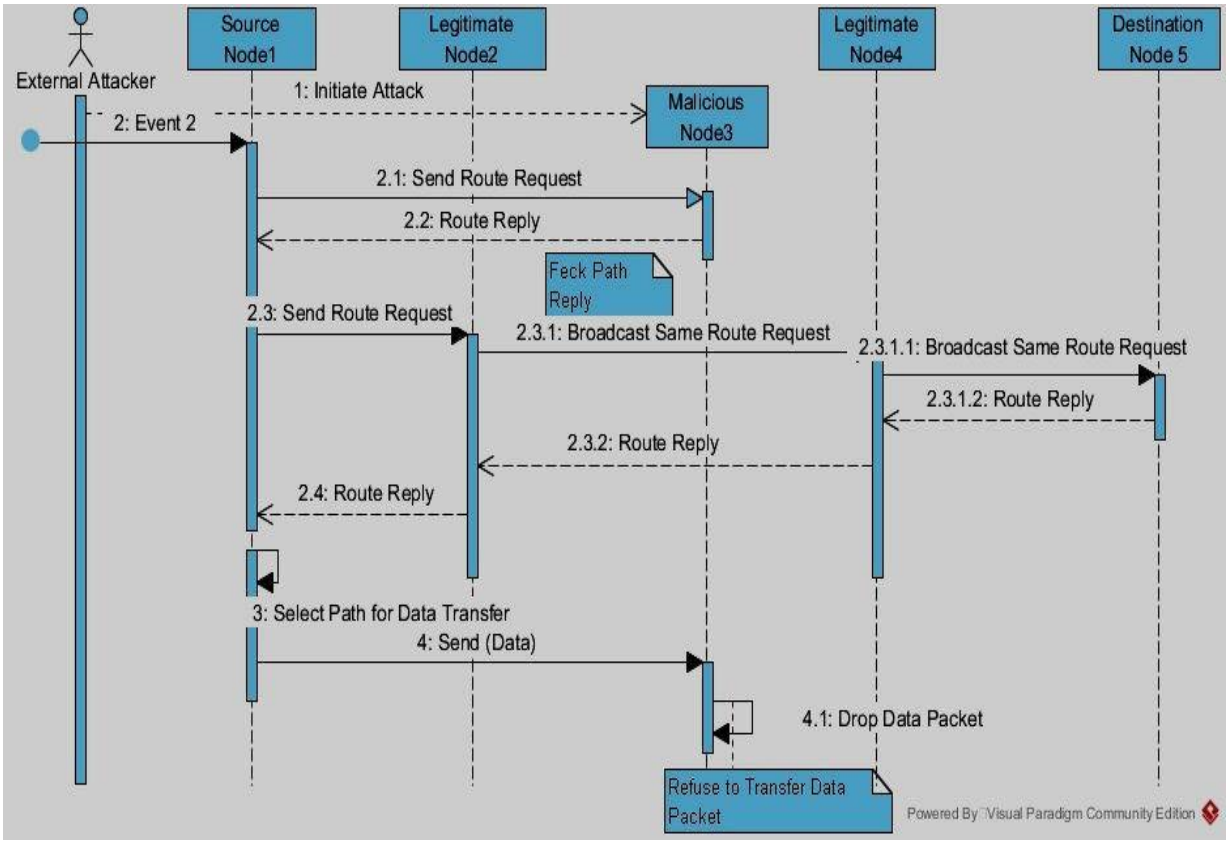

Fig.1UML Sequence Diagram for Black Hole Attack

B. *GRAY HOLE ATTACK*

Gray Hole is a special type of Blackhole attack. In which malicious node switches its state back and forth authentic to malicious [1].Recognition of GrayHole attack is harder because, in contrast to Black Hole attacks where all packets drop, a Gray Hole attack drops only a subset of the packets and is thus more difficult to detect. Also, the attacker may drop the packets arbitrarily or according to any distribution. In a multi-hop network, it is difficult to distinguish a random packet drops caused by a Gray Hole attack from those caused by congestion.
A Gray Hole node may reveal its malicious behavior in several ways:-
(i) It can drop packets with specific probability coming from certain nodes while forwarding packets from other nodes correctly.
(ii) It can drop packets only for predefined time duration but may switch back to normal routing behavior later.
(iii) It can combine the latter two scenarios

The detailed procedure is as follows below in Fig.2

1) An attacker compromises a malicious node 3 and initiates for gray hole attack
2) Source node1 detects an event to establish a route to destination node5.
3) Source node1 broadcast route request to search for destination node5.
4) Malicious node3 receives and broadcast same request.
5) (source node1→ malicious Node3→ legitimate node4→ destination node5)

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

6) Source node select route via malicious node and send data packet.
7) The malicious node receives data packet then check for the particular condition if condition satisfies then forward the data packet to next hop (legitimate node4) Else drop the received data packet.

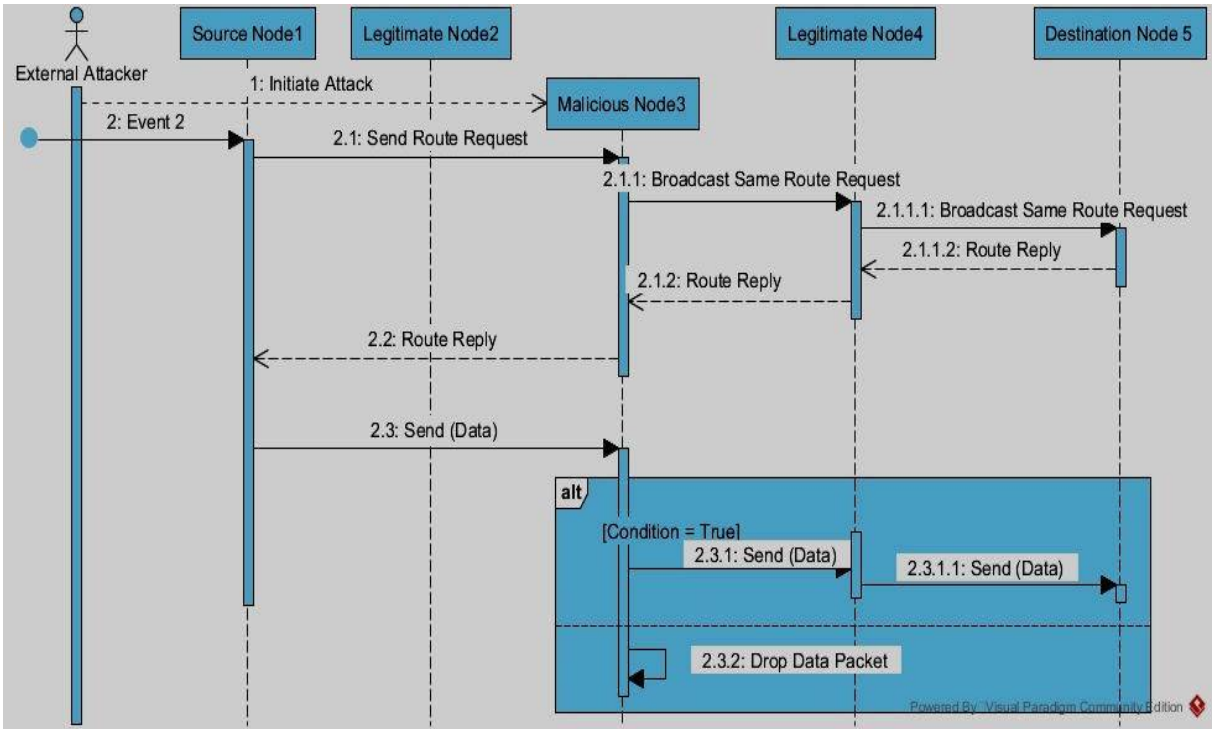

Fig.2 UML Sequence Diagram for Gray Hole Attack

C. *WORM HOLE ATTACK*

Two or more malicious nodes launch a wormhole attack using a private channel called tunnel, between them. At one end of the tunnel, a compromised node captures a control packet and sends it to another colluding node at the other end through a private channel, which rebroadcasts the packet locally. The attack normally works in two phases. In the first phase, the wormhole nodes get themselves involved in several routes. In the second phase, these malicious nodes start exploiting the packets they receive. These nodes can disrupt the network functionality in a number of ways. Wormhole nodes can drop, modify, or send data to a third party for malicious purposes.

The detailed procedure is as follows below in Fig.3

1) An attacker compromises a malicious node 2 and malicious node4.Create a tunnel between them.
2) Source node1 generates an event, send data packet to destination node5.
3) Malicious node2 receives a data packet from its neighbor node and then forwards that packet trough tunnel to malicious node4.
4) Malicious node4 replays data packet.
5) (source node1→ malicious Node2→ malicious node4→ malicious gateway)

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

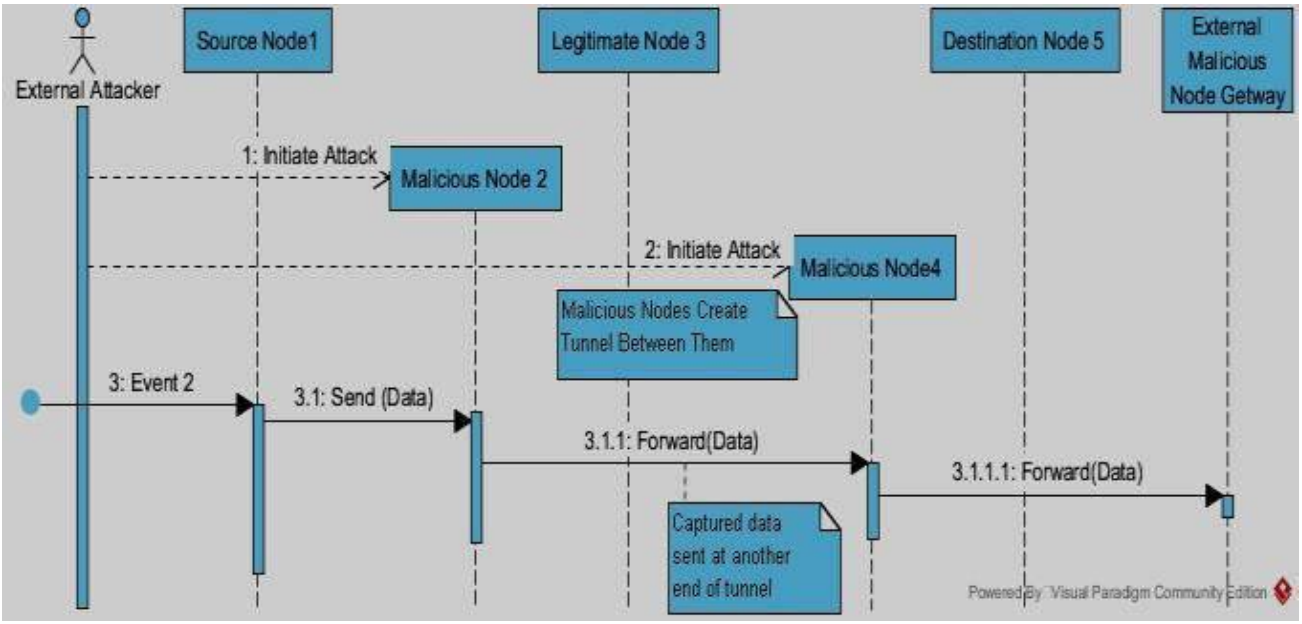

Fig.3UML Sequence Diagram for WormHole Attack

D. *SYBIL ATTACK*

In Sybil attack, attacker compromise authentication property of MANET. Sybil attacker may produce bogus identities of a number of additional nodes. In this, a malicious node pretends itself as an enormous number of nodes instead of a single node. The additional identities that the node obtains are called Sybil nodes. A Sybil node may formulate a new identity for itself, or it steals an identity of the authentic node.

The detailed procedure is as follows below in Fig.4

1) An attacker compromises a malicious node3 and initiates for Sybil attack.
2) Malicious node3 send a hello message with different identities to its neighbors.
3) Malicious node may generate fake identities or steal from legitimate node
4) Legitimate nodesnode1, node2 and node3 listen and update their routing table. In this attack authenticity requirement of MENT is spoiled.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

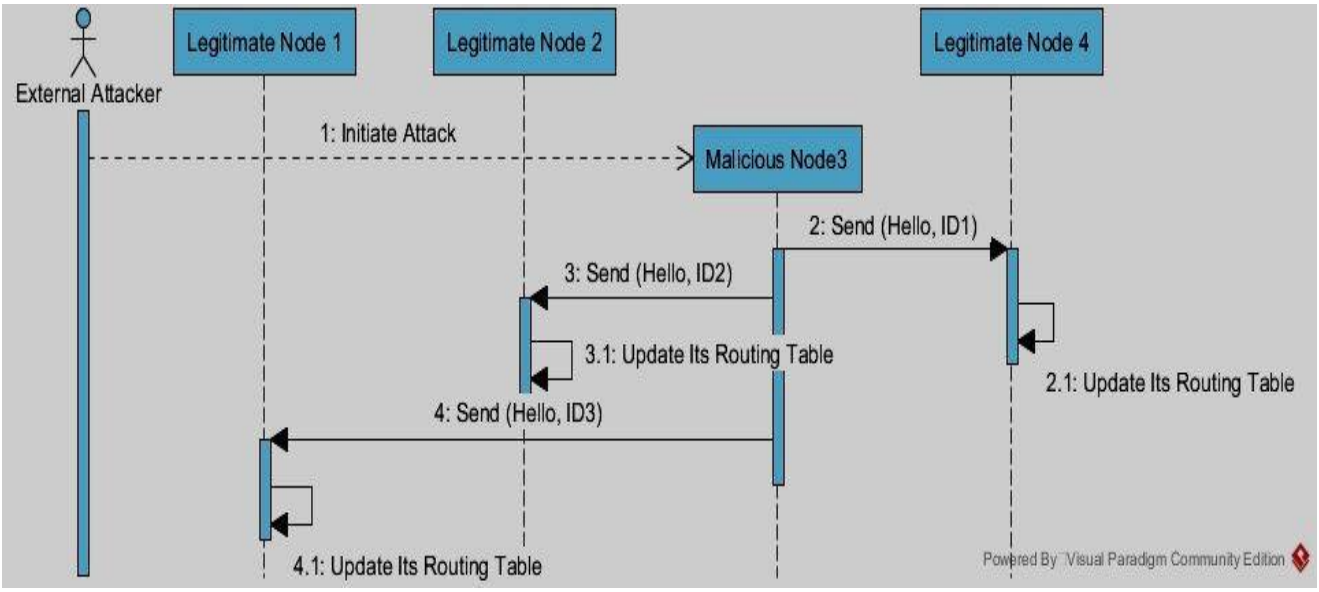

Fig.4 UML Sequence Diagram for Sybil Attack

E. *JELLYFISH ATTACK*

Jellyfish attack is a sort of passive attack. In Jellyfish attack attacker purposely produces a delay in transmission and reception of data packets in the network. As a result, themessage cannot reach the destination within the hard deadline. This attack is difficult to detect. Sometimes messages are recorded or stored at the compromised node. Jellyfish attack further classified into three subcategories Jellyfish recorder attack, Jellyfish periodic dropping attack and Jellyfish Delay variance attack [3].
The detailed procedure is as follows below in Fig. 5

1) An attacker compromises a malicious node3 and initiates for jelly fish attack
   Source node1 detects an event to forward data to node2 that is on the routing path.
   (Source node1→ legitimate node 2 → malicious Node3→ legitimate node4→destination node3)
2) Malicious node3 receives data from node2 and generates delay before transmitting data to next hop node.
   (Source node1→ node2→ malicious Node3-----→ node 4→ destination node

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

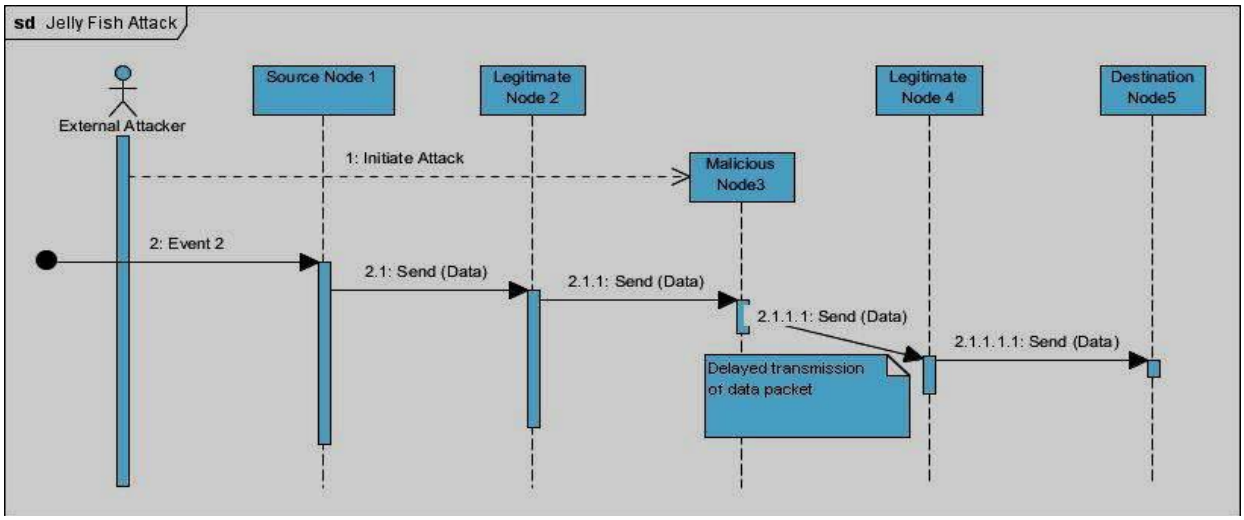

Fig.5 UML Sequence Diagram for Jelly Fish Attack

F. *SLEEP DEPRIVATION ATTACK*

Sleep deprivation (SD) is also known as resource consumption attack. The aim of an intruder here is to drain off limited resources in the MANET nodes by constantly making them busy in processing unnecessary packets [1].Sleep deprivation attacks can be launched by flooding unnecessary routing packets to the targeted node. For example, attacker broadcasts a large number of RREQ messages in route discovery phase.So all other legitimate nodes receive them and end up reducing their battery power while processing the received RREQs.
The detailed procedure is as follows below in Fig.6

1) An attacker compromises a malicious node3 and initiates for Sleep Deprivation attack.
2) Malicious node3 send a route request to legitimate node2 and legitimate node4, which are in its range.
3) Node2 and Node4 broadcast the same request.
4) Malicious node continuously repeats step 2and3.

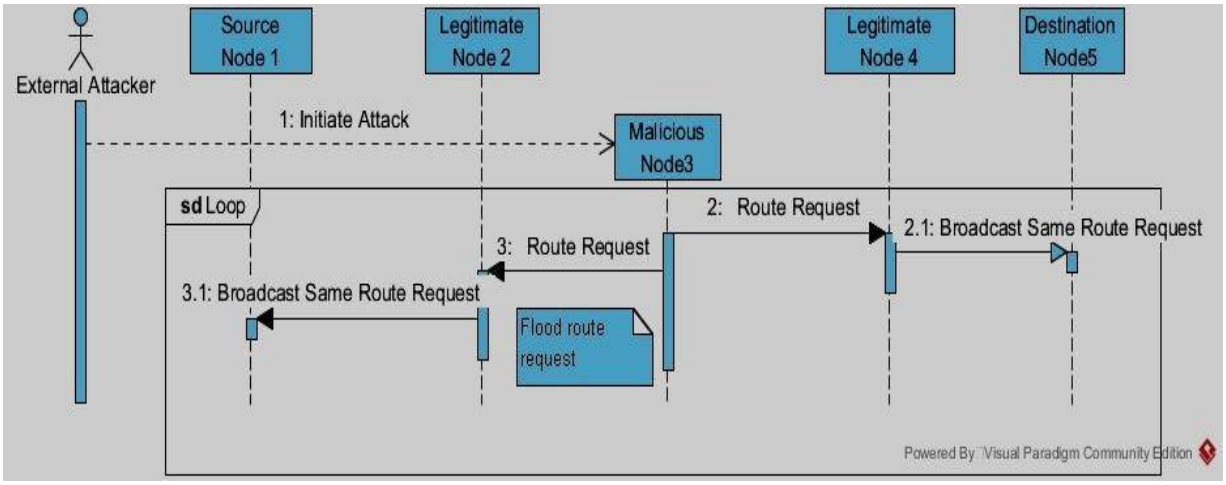

Fig.6 UML Sequence Diagram for SleepDeprivation Attack

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

G. *BYZANTINE ATTACK*

In this attack, the aim of the intruder is to disturb the network service and degrade the performance of the network. A compromised node works alone, or a group of compromised nodes work together and perform activities such as creating loops in routing path, packets forwarding through non-optimal paths, or dropping packets selectively [4].

The detailed procedure is as follows below in Fig.7

1) AnattackercompromisesamaliciousnodeandinitiatesforByzantineattack.
2) Sourcenode1detects an event to forward data to node2 that is on the routing path.(Source node1→legitimate node2→ malicious Node3→ legitimate node4→ destination node5)
3) On receiving data from the node,two malicious node alter the routing path. Creates loop (node3→ node2→nodes1)
4) Node 2 forwards the received data from node3 to node1 according to the altered routing path. Repeat steps2 thru step3.

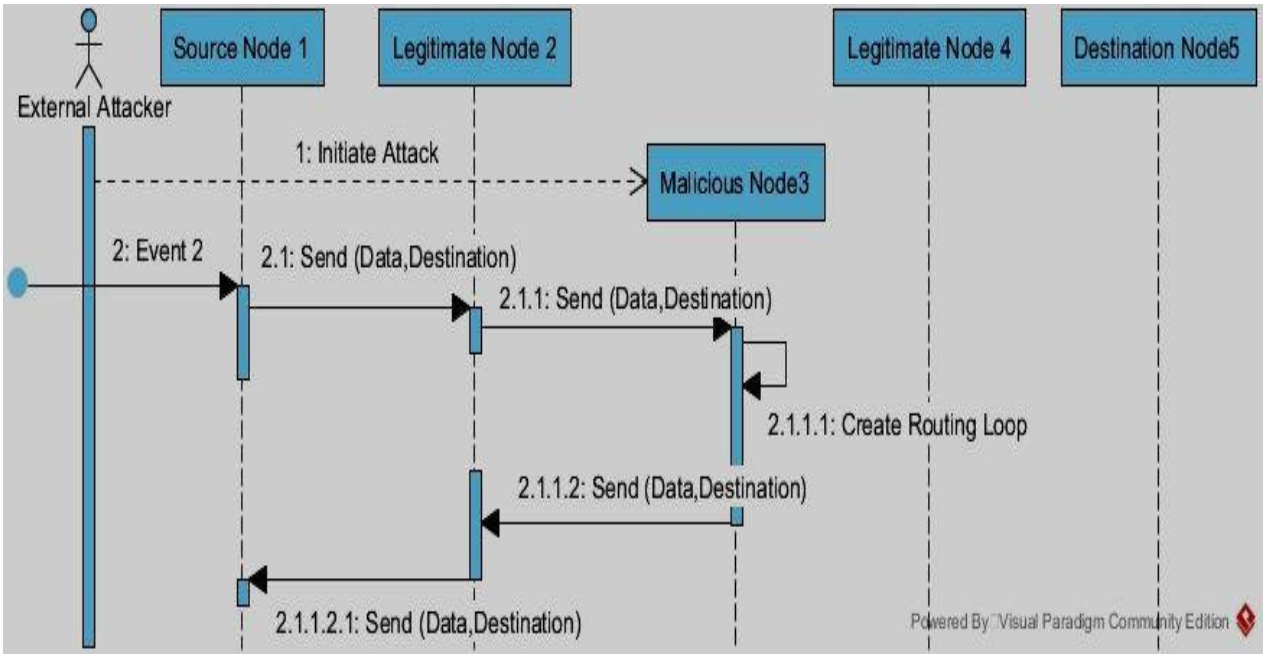

Fig.7 UML Sequence Diagram for Byzantine Attack

IV. CONCLUSION AND FUTURE WORK

MANET used for military operation, or in a rescue operation like a flood, earthquake, etc. The main requirement of these applications is security. Due to intrinsic features of Ad-hoc network, MANET is more prone to security threat like a Blackhole, gray hole, sleep deprivation, wormhole attack. To protect MANET from an intruder, security attacks must be well studied to find countermeasures. In this paper, well-known network layer security attacks are modelled using a sequential diagram**.** This work provides a better understanding of attacks; it helps the developer to build more secure MANET.

From the so far discussion, it is clear that MANETs are an easy host for several types of attacks. A black hole is one of the renowned securities attacks in MANET in which attacker abuse the weakness of Reactive Routing Protocol. Compromised node advertises itself as having the short and fresh route to the destination and drops the receiving packets.

As a future work, designing a Black Hole detection and prevention system that effectively detects and prevents the Black Hole attack in any environment while keeping the minimum overhead will be the focus.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 10, October 2016

REFERENCES

1. Adnan Nadeem and Michael P.Howarth, "A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks", IEEECommunicationsSurveys&Tutorials,Vol.15, PP.2027-2045,2013
2. A.Saeed, A.Razaand and H.Abbas, "A Survey on Network Layer Attack And AODV Defense in Mobile Ad hoc Networks", Eighth International Conference on Software Security and Reliability – Companion,PP.185-191,2014
3. R.Ranjan, N.Singh, and A.Singh, "Security Issues of Black Hole Attacks in MANET",Int. Conf. on Computing, Communication & Automation(ICCCA), PP.452-457,2015
4. A.Abdelaziz, M. Nafaaand G. Salim, "Survey of Routing Attacks and Countermeasures in Mobile Ad Hoc Networks,"IEEE(UKSim),PP.693-698,2013
5. Sunghyuck Hong, Sunho Limand JaekiSong' "Unified Modeling Language based Analysis of Security Attacks in Wireless Sensor Networks: A Survey", KSII Transactions on Internet and Information Systems, VOL. 5, NO. 4, PP. 805-821 , April 2011
6. Sunghyuck Hong and SunhoLimt, "Analysis of Attack Models via Unified Modeling Language in Wireless Sensor Networks: A Survey Study", IntConf on Wireless Communication ,Networking and Information Security, PP.692-696, 2010
7. Pranav M. Pawar, RasmusH.Nielsen, NeeliR.Prasad , Shingo Ohmori and RamjeePrasad", Behavioral Modelling of WSN MAC Layer Security Attacks:A Sequential UMLApproach", Journal of Cyber Security and Mobility, PP. 65–82 ,2012
8. PallaviKhatri ,SaritaBhadoria, and MamtaNarwariya, "A Survey on Security issues in MobileADHOC networks", International Journal of Computing Science and Communication Technologies, VOL. 2, NO. 1, PP.229-233, July 2009
9. PriyankaGoyal, VintiParmar, Rahul Rishi, "MANET: Vulnerabilities, Challenges, Attacks, Application", IJCEM International Journal of Computational Engineering & Management, Vol. 11, PP.32-37, January 2011
10. S. Balasubramani, S.K. Rani and K. SujaRajeswari, "Review on Security Attacks and Mechanism in VANETand MANET ", S.S. Dash et al. (eds.), Artificial Intelligence and Evolutionary Computations in Engineering Systems, Advances in Intelligent Systems and Computing 394, © Springer India 2016.
11. Rajakumar P, PrasannaVenkatesan T, Pitchaikkannu A, "Security Attacks And Detection Schemes In MANET", Int. Conf. Electron CommunSyst (ICECS), PP. 1–6. 2014;
12. Amitabh Mishra, "Security and Quality of Service in Ad Hoc Wireless Networks" (chapter 1, 3), ISBN- 13 978-0-521-87824-1 Handbook.