Opinder Singh *et al*, International Journal of Computer Science and Mobile Applications,
Vol.4 Issue. 6, June- 2016, pg. 80-85 **ISSN: 2321-8363**
Impact Factor: 4.123

FLOODING ATTACK COUNTERMEASURES IN MOBILE ADHOC NETWORKS

Opinder Singh[†], Dr. Jatinder Singh[‡], Dr. Ravinder Singh[‡]

[†]Research Scholar, IKG PTU, Kapurthala, Punjab.
[‡]IKG PTU, Kapurthala, Punjab.
E-mail: [†] opindermca2008@gmail.com, [‡] bal_jatinder@rediffmail.com, [‡] dr.rs.global@gmail.com

Abstract: ***A mobile adhoc network (MANET) is an infrastructure-less type network, which consists of number of mobile nodes with wireless network interfaces. In MANET every node functions as transmitter, router and data sink. MANET has dynamic topology which allows nodes to join and leave the network at any point of time. MANET is more vulnerable due to its characteristics such as dynamic topology, distributed cooperation and open medium. Security issues in mobile adhoc networks are veiled by various techniques that were introduced in past decade. Due to decentralized nature of MANET, the security issues cultivate resulting in welcoming various lethal vulnerabilities. Out of all attacks in MANET, Flooding attacks are considered most challenging adversarial modules that tremendously affect the communication system in MANET. This paper presents survey of various security techniques used for mitigating Flooding attacks in MANET.***

Keywords: Mobile ad hoc network (MANET), Security, vulnerabilities, Attacks, Flooding attack, Intrusion Detection Systems.

1. Introduction

Mobile Ad hoc Networks (MANET) are the wireless networks of mobile computing devices without any support of a fixed infrastructure. The mobile nodes in a MANET self organize together in some arbitrary fashion. A MANET is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. These networks can be applied between persons or between vehicles in areas which are depleted of fixed infrastructure. Two nodes can directly communicate with each other if they are within the radio range. If the nodes are not within the radio range they can communicate with each other using multi hop routing. The wireless link between the nodes in mobile networks is highly vulnerable. This is because nodes can continuously move causing the frequent breakage of the link. The power available for transmission is also strictly limited. The topology of the network is highly dynamic due to the continuous breakage and establishment of wireless link Nodes continuously move into and out of the radio range. This gives rise to the change in routing information. The network is decentralized; where all network activity including discovering the topology and delivering messages must be executed by the nodes themselves i.e. routing functionality will be incorporated into mobile nodes.

Opinder Singh *et al*, International Journal of Computer Science and Mobile Applications,
Vol.4 Issue. 6, June- 2016, pg. 80-85 **ISSN: 2321-8363**
Impact Factor: 4.123

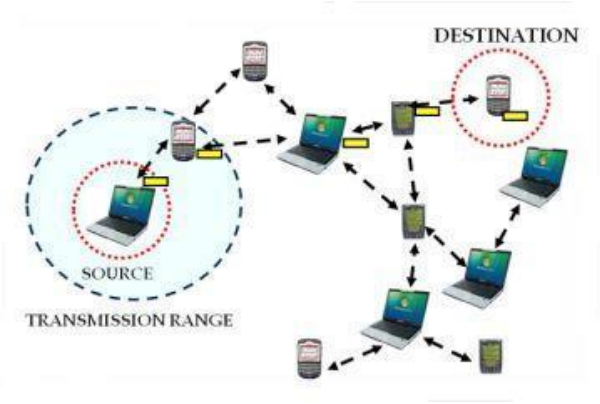

Fig.1. Mobile Ad hoc network.

MANET is more vulnerable than wired network due to mobile nodes, threats from malicious nodes inside the network. Because of vulnerabilities, MANET is more prone to malicious attacks. MANET has following vulnerabilities [1, 2]:

- Lack of centralized node
- Scalability
- Limited power supply
- Adversary inside the Network
- Limited Resources
- Dynamic topology
- Bandwidth constraint
- No predefined Boundary

MANET often suffer from security attacks because of its features like open medium, dynamic topology, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battle field situation for the MANET against the security threats. Various attacks on different layers of MANET are shown in the following figure.

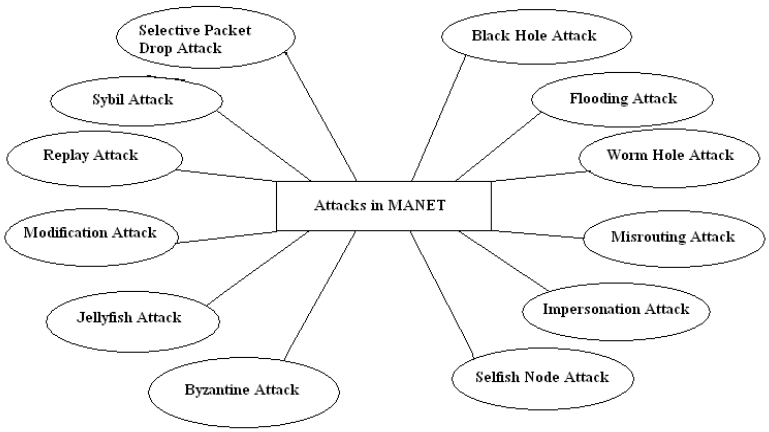

Fig.2. Different types of attacks in Mobile Ad hoc network.

1.1 Flooding Attack

The flooding attack is easy to implement but cause the most damage. This kind of attack can be achieved either by using RREQ or Data flooding. In RREQ flooding the attacker floods the RREQ in the whole network which takes a lot of the network resources. This can be achieved by the attacker node by selecting such I.P addresses that do not exist in the network. By doing so no node is able to answer RREP packets to these flooded RREQ. In data flooding the attacker get into the network and set up paths between all the nodes in the network. Once the paths are established the attacker injects an immense amount of useless data packets into the network which is directed to all the other nodes in the network. These immense unwanted data packets in the network congest the network. Any node that serves as destination node will be busy all the time by receiving useless and unwanted data all the time. The aim of the flooding attack is to exhaust the network resources: bandwidth and to consume a node's resources, such as battery power and computational or to disrupt the routing operation to cause severe degradation in network [4, 6].

2. Flooding Attack Countermeasures

In this section of the paper, we provide various countermeasures proposed in the literature to tackle with the flooding attack in mobile adhoc networks.

A. Trust Based Mechanism

Shishir K. Shandilya and Sunita Sahu in their paper entitled "A Trust Based Security Scheme for RREQ Flooding Attack in MANET" proposed a novel technique to detect the flooding attack in MANET. This technique is based on the trust mechanism. Trust of the whole network is calculated based on the trust estimation function in DSR on demand routing protocol. This trust based mechanism is a distributive approach to detect and prevent flooding attack. The concept of this technique depends upon the threshold values. The concept of delay queue in this method reduces the probability of accidental blacklisting of the node but it also delays the detection of misbehaving node by allowing him sends more packet until delay queue time out occurs. This mechanism is used to detect and mitigating RREQs flooding attack and the proposed method can be extended to prevent data flooding also [7].

B. Dynamic Profile Based Technique

Sathish and Sasikala in their paper entitled "Dynamic Profile Based Technique to Detect Flooding Attack in MANET" developed a dynamic profile based mechanism to detect and mitigate flooding attack in MANET using AODV protocol. In this approach, every node is set with some profile for encountering the distributed attack. The profile values are set on the basis of behavior of MANET. This mechanism is used to identify and isolate the attack whenever the node cross the defined threshold value. This threshold value is based on the average request allowed in the network. Furthermore, another distinguishable contribution made by this DPDS is that it can identifyThis mechanism is different as this approach is also capable of finding impact of attack on the MANETs. The advantage of this approach is that it detects the malicious nodes at one hop neighbor level as soon as they start exhibiting the attack behavior. DPDS efficiently detects and isolates the attacker node as compared to rate limit approach. Response time and detection rate are also improved by using this approach. This approach also helpful in preventing the resource consumption attack. In future this mechanism can be extended for other kind of attacks with respect to AODV protocols [8].

C. Hierarchical cluster based

D. Srinivasa Rao and Dr. P.V. Nageswara Rao in their paper entitled "An Efficient RREQ Flooding Attack Avoidance Technique for Adaptive Wireless Network" provide a hierarchical cluster based mechanism for detecting and mitigating RREQ flooding attack in MANETs. This approach is used to reduce the impact of flooding attack on the performance of MANET. Due to hierarchical cluster based approach this technique is unique in terms of route security and dynamic adaptability. In this mechanism each node in the network is able to detect attacker node because all of the communication will happen through cluster head whether both source and the destination node are in same cluster or in other cluster. In this technique each node does not need to continuously observe

the behavior of the neighbor node. The simulation result shows that this technique gives better performance under Packet Delivery Ratio, Routing Overhead and Throughput [9].

D. Distributive approach

Ms. Neetu Singh Chouhan and Ms. Shweta Yadav in their paper entitled "Flooding Attacks Prevention in MANET", proposed a distributive approach for detecting and preventing flooding attack in MANETs. This mechanism is used for detecting a new type of attack known as Adhoc Flooding Attack(AHFA) in mobile adhoc networks under AODV. The effectiveness of the proposed technique depends on the selection of threshold values. In this technique when the intruder broadcasts large number of packets of Route Request, the immediate neighbors of this node notice the behavior of this node and check its trust by a trust function . Once the threshold value is exceeded at the same time nodes deny any future request packets from this node. The concept of delay queue used in this technique reduces the probability of accidental blacklisting of the node. The results of this implementation show that distributive approach can prevent the Ad Hoc Flooding attack efficiently. Future work of this research can be optimise value of threshold and improve their performance [10].

E. Assumptions and Attacker Model

Venkat Balakrishnan, Vijay Varadharajan, and Uday Tupakula in their paper entitled "Mitigating Flooding Attacks in Mobile Ad-hoc Networks Supporting Anonymous Communications" proposed an assumptions and attacker model for mitigating flooding attacks in MANETs. This technique is capable of efficiently identifying and isolating the malicious node that floods route request in the network. This approach is also capable of identifying the benign behavior of an expelled node and an expelled node can also rejoins back into the network. This technique also not require any additional packets to communicate the behavior of the flooding node, so additional overhead can be reduced. In this mechanism it is assumed that the nodes can communicate using a single shared bi-directional wireless channel and all the transmissions and receptions are omni-directional. The simulation results confirm about these characteristics and hence this technique seems to be very promising for counteracting flooding attacks in mobile ad hoc networks supporting anonymity The main advantages of this technique is that it can efficiently identify and eliminate the nodes that are flooding in the mobile adhoc networks [11].

F. Effective filtering scheme

Jian-Hua Song, , Fan Hong and Yu Zhang in their paper entitled "Effective filtering Scheme against RREQ Flooding Attack in Mobile Ad Hoc Networks" proposed a new scheme for preventing against RREQ flooding attack. This technique is based on an Effective Filtering scheme. This mechanism can detect the malicious nodes and attacker nodes, which are flooding route request in the network communication. In this scheme two thresholds are used in order to limit the RREQ message and these are: 1) RATE_NM and 2) BLACKLIST_NM. RATE_NM parameter denotes no. of RREQ that can be accepted and processed. In this technique each node in the network monitors the RREQ and maintain a count table for RREQ received. Everytime when a RREQ is received a condition check is performed by the node. If the rate of received RREQ is less than the RATE_NM then received RREQ processed as normal otherwise a second condition check is performed, where received RREQ is compared with another threshold BLACKLIST_NM, if the rate of RREQ is greater than the BLACKLIST_NM then it is assume that the node is trying to flood the network with fake RREQ messages otherwise the received RREQ is add to delay queue. After adding malicious node to blacklist all the neighboring nodes of malicious node now free to entertain RREQ from other genuine nodes, if the received RREQ has rate in between RATE_NM and BLACKLIST_NM then this will de add to delay queue. By doing so the node which has high attack rate will be delayed [12].

3. Research Gaps

- Most of the research in the past for detecting flooding attack has been carried out on distributed based mechanisms but a little work is done on threshold based mechanisms. So, work need to be done for fulfilling this research gap.
- There is a lot of research gap for developing an efficient mechanism for tackling with flooding attack in AODV protocols based on statistical methods.
- Most of the work has been carried out for tackling with flooding attack is based on cumulative acknowledgement encryption mechanism, hashing mechanism but design of an efficient mechanism still remains a challenge.

The exact design consideration for efficient technique for monitoring, detecting and responding to flooding attack in MANET has not been accounted so for according to authors' knowledge.

4. Conclusion and future work

The applications of mobile adhoc networks are increasing along with the need for more effective security mechanisms. The security concerns of the MANETs should be addressed from the beginning of designing of the system. A thorough understanding of the capabilities and limitations of each of underlying technology is required for the secure working of mobile adhoc networks. In this paper we first discuss the flooding attack in detail and then we provide in detail different techniques / mechanisms proposed for tackling with flooding attack in the literature. A thorough study of limitations of available techniques will help in the design of novel, robust, and secure mechanism against flooding attack, so that the mobile adhoc networks applications can be extended to other fields. More development and deployment of defense mechanisms from researchers and service providers respectively is what we expect to see in the near future.

5. ACKNOWLEDGEMENT

Authors are highly thankful to the Department of RIC, IKG Punjab Technical University, Kapurthala, Punjab, India for providing opportunity to conduct this research work.

References

[1] Sachin Lalar, "Security in MANET: Vulnerabilities, Attacks & Solutions", "International Journal of Multidisciplinary and Current Research", Volume 2, Jan-Feb, 2014, ISSN: 2321-3124.
[2] Jatinder Singh, Lakhwinder Kaur, and Savita Gupta, "A Cross-Layer Based Intrusion Detection Technique for Wireless Networks", "International Arab Journal of Information Technology", Volume 9, No. 3, May 2012 and ISSN: 1683-3198.
[3] P. K. Singh and G. Sharma, "An Efficient Prevention of Black Hole Problem in AODV Routing Protocol in MANET", "IEEE International Conference on Trust, Security and Privacy in Computing and Communications", 2012.
[4] Gagandeep, Aashima, Pawan Kumar, "Analysis of Different Security Attacks in MANETs on Protocol Stack A-Review", International Journal of Engineering and Advanced Technology (IJEAT), , Volume-1, Issue-5, June 2012 and ISSN: 2249 – 8958.
[5] Satria Mandala, Md. Asri Ngadi, A.Hanan Abdullah, "A Survey on MANET Intrusion Detection", "International Journal of Computer Science and Security", Volume 2, Issue 1, 2013 and ISSN:1985-1553.

[6] Sandip Nemade, Manish Kumar Gurjar, Zareena Jamaluddin, Nishanth **,**"Early Detection of Syn Flooding Attack by Adaptive Thresholding (EDSAT): A Novel method for detecting Syn Flooding based DOS Attack in Mobile Ad Hoc Network", "International Journal of Advanced Research in Engineering and Technology (IJARET)", Volume 5, Issue 2, February (2014), ISSN 0976 – 6480(Print), ISSN 0976 – 6499(Online).
[7] Shishir K. Shandilya and Sunita Sahu, "A Trust Based Security Scheme for RREQ Flooding Attack in MANET", International Journal of Computer Applications (0975 – 8887) Volume 5– No.12, August 2010.
[8] Sathish and Sasikala, "Dynamic Profile Based Technique to Detect Flooding Attack in MANET", "International Journal of Innovative Research in Computer and Communication Engineering", Vol.2, Issue 1, March 2014, ISSN(Online): 2320-9801, ISSN (Print): 2320-9798.
[9] D. Srinivasa Rao, Dr. P.V. Nageswara Rao, "An Efficient RREQ Flooding Attack Avoidance Technique for Adaptive Wireless Network", "International Journal of Applied Engineering Research", Volume 11, 2016, ISSN 0973-4562.
[10] Ms. Neetu Singh Chouhan and Ms. Shweta Yadav, "Flooding Attacks Prevention in MANET", "International Journal of Computer Technology and Electronics Engineering (IJCTEE)", Volume 1, Issue 3, ISSN 2249-6343.
[11] Venkat Balakrishnan, Vijay Varadharajan, and Uday Tupakula in their paper entitled "Mitigating Flooding Attacks in Mobile Ad-hoc Networks Supporting Anonymous Communications"
[12] Jian-Hua Song, , Fan Hong, Yu Zhang, "Effective filtering Scheme against RREQ Flooding Attack in Mobile Ad Hoc Networks", IEEE Computer Society 2006.
[13] Revathi Venkataraman, M. Pushpalatha, and T. Rama Rao, "Performance Analysis of Flooding Attack Prevention Algorithm in MANETs", International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol:3, No. 8, 2009.
[14] Jerome François, Issam Aib and Raouf Boutaba, *"FireCol*: A Collaborative Protection Network for the Detection of Flooding DDoS Attacks", "IEEE/ACM TRANSACTIONS ON NETWORKING", VOL. 20, NO. 6, DECEMBER 2012.
[15] Jin Tang, Yu Cheng and Yong Hao,"Detection and Prevention of SIP Flooding Attacks in Voice over IP Networks", "IEEE INFOCOM,2012", ISSN-978-1-4673-0775.
[16] Saman Taghavi Zargar, James Joshi and David Tipper, "A Survey of Defense Mechanisms Against Distributed Denial of Service (DDoS) Flooding Attacks", "IEEE COMMUNICATIONS SURVEYS & TUTORIALS", VOL. 15, NO. 4, FOURTH QUARTER, 2013.
[17] Jin Tang, Yu Cheng, Yong Hao, and Wei Song, "SIP Flooding Attack Detection with a Multi-Dimensional Sketch Design", "IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING", VOL. 11, NO. 6, NOVEMBER/DECEMBER 2014.
[18] Jaehak Yu, Hyo-Chan Bang, H. Kang, D. Park, "An in-depth analysis on traffic flooding attacks detection and system using data mining techniques", "Journal of Systems Architecture: the EUROMICRO Journal", Volume 59, Issue 10, November, 2013.

