# COUNTERMEASURES AGAINST SELECTIVE PACKET DROP ATTACK IN MOBILE ADHOC NETWORKS: A SURVEY

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

[†] *Research Scholar, IKG PTU, Kapurthala, Punjab.*
[‡,#]*IKG PTU, Kapurthala, Punjab.*
[†]opindermca2008@gmail.com,[‡]bal_jatinder@rediffmail.com,[#] dr.rs.global@gmail.com

***ABSTRACT***
***A MANET is an infrastructure-less 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. Various techniques are deployed to resolve different security issues and challenges in MANETs, but due to dynamic nature of MANETs the security techniques are still unable to prevent the network completely. MANETs are more vulnerable to various types of network attacks. Out of different attacks Selective Packet Drop attack is considered as one of the most dangerous attack which drops the packets randomly. This paper presents various security techniques used for mitigating Selective Packet Drop attacks in MANET. The study also highlights some of the significant findings as well as research gap that can be used as prime contribution for the proposed paper.***
***Keywords: Mobile ad hoc network (MANET), Security, vulnerabilities, Attacks, Selective Packet Drop attack, Intrusion Detection Systems.***

## I. 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

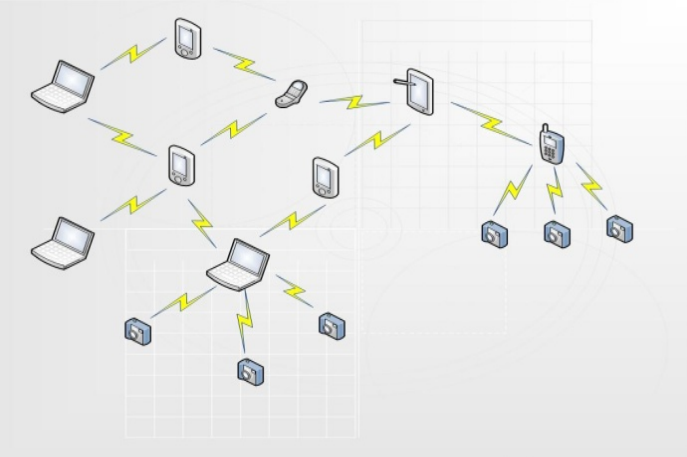

**Fig.1.** Mobile Ad hoc network

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 mobilenodes. 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
- 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 [3,4]. Various attacks on different layers of MANET are shown in the following figure.

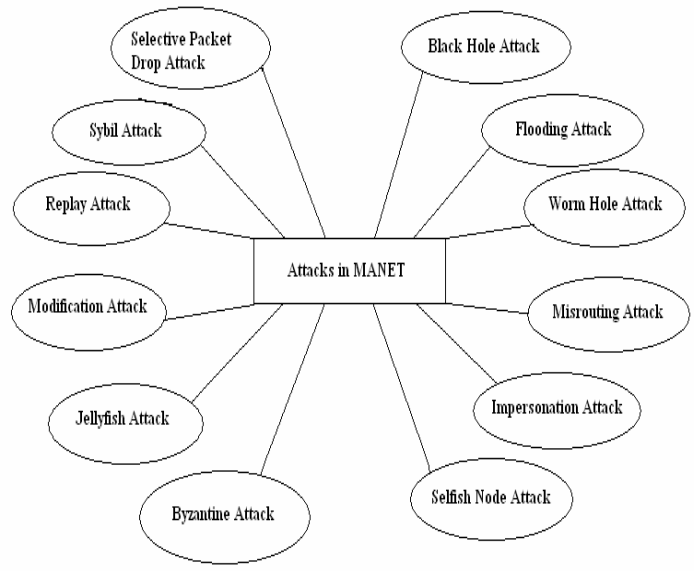


**Fig.2.** Different types of attacks in Mobile Ad hoc network

Out of different attacks Selective Packet Drop attack is considered as one of the most dangerous attack which drops the packets randomly.

### *1.1 Selective Packet Drop Attack*

In a black hole attack, compromised node drops all the packets forwarding through it. A special case of black hole attack is Selective packet drop attack, where compromised node drop packets selectively, which may deteriorate the network efficiency. Another name of this type of attack is Selective forwarding attack. In this type of attack malicious nodes behave like normal nodes in most time but selectively drop sensitive packets for the application. Such selective dropping is hard to detect. Selective packet drop attacks are the attacks which may corrupt some mission critical applications such as military surveillance and forest fire monitoring [6,7]. The malicious nodes behave like normal nodes in most time but selectively drop some sensitive packets.

## II. BRIEF LITERATURE SURVEY

A variety of literature is available related to intrusion detection in MANET for Selective packet drop attacks. A few of the related work is discussed below:

1] Archana and Maya Mohan in their paper entitled “An Intrusion Detection System for MANET against Selective Packet Dropping” proposed a robust trust-aware IDS to tackle with selective packet drop attack and help in reducing routing overhead and delay caused by EAACK. The proposed intrusion detection system is efficient as compare to EAACK in case of same attack in MANET and produces less RO and delay. By using this type of IDS network overhead and packet dropping is reduced by considering association between different nodes in MANET. Simulation results show that robust trust-aware IDS is efficient as compare with EAACK in case of same attack under different parameters [8].

[2] Anita and Abhilasha in their paper entitled “A Novel Technique to Protect and Isolate Selective Packet Drop Attack in MANET”, proposed a novel technique based on the Diffie-Hellman algorithm to reduce packet drop problem by detecting and isolating selective packet drop attack in MANET.By this technique throughput of the whole network will be improved. This Diffie- Hellman algorithm based technique is also responsible for less packet delay and less packet loss as compare to other techniques [9].

[3] N.Bhalaji and Dr. A.Shanmugam in their paper entitled “Reliable Routing against Selective Packet Drop Attack in DSR based MANET” proposed dynamic trust based approach to detect and isolate selective packet drop attack in MANET. Simulation results of this technique shows that this new routing mechanism is much better than other conventional techniques used for isolating selective packet drop attack in MANET. Other conventional techniques are usually based on encryption and hashing mechanisms. These techniques are only suited for planned networks. For network like MANET dynamic trust based technique is much better than existing techniques. This dynamic trust based technique is also responsible for identifying and isolating the malicious nodes from the active data routing and forwarding [10].

[4] Ming Yang Su in his paper entitled "Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems" proposed a new technique to detect and separate malicious nodes, which selectively perform black hole attacks by deploying IDSs in MANETs (mobile ad hoc networks). All IDS nodes perform an ABM (Anti-Black hole Mechanism), which estimates the suspicious value of a node, according to the amount of abnormal difference between RREQs and RREPs transmitted from the node. With the prerequisite that intermediate nodes are forbidden to reply to RREQs, if an intermediate node, which is not the destination and never broadcasts a RREQ for a specific route, forwards a RREP for the route, then its suspicious value will be increased by 1 in the nearby IDS’s SN (suspicious node) table. When the

suspicious value of a node exceeds a threshold, a Block message is broadcasted by the detected IDS to all nodes on the network in order to cooperatively isolate the suspicious node. Even if the numbers of IDSs are not enough to cover most of the area, the proposed IDS can perform very well because this IDS can reduce total packet loss rate in the MANET [11].

[5] Shah Vrutik, Dr. NileshModi, PataniAshwin in their paper entitled " AODVGAP-An Acknowledgment based approach to mitigate selective forwarding attacks in MANET" proposed a security mechanism for selective forwarding attacks in MANET named as gray hole Attack Prevention (GAP). They analyzed effect of the Gray Hole in an AODV Network. Gray hole Attack Prevention (GAP) is to fortification of Selective packet forwarding attack (Gray hole attack) on well known Reactive routing protocol Ad-Hoc on Demand Distance Vector (AODV). Simulation has been done using ns 2.34 to evaluate the conventional AODV and AODV-GAP when selective packet drop attack is injected in network. The Result indicates that their proposed solution gives significant better performance in concern of Packet delivery ratio & Throughput with tolerable increase in routing overhead, End to End delay [12]. In future this technique can be extended to prevent from flooding attacks.

[6]Jui-Pin Yang, Yuan-Sun Chu, and Ming-Cheng Liang in their paper entitled "Threshold-Based Selective Drop for Shared Buffer Packet Switches" proposed a novel buffer management scheme called threshold-based selective drop (TSD) to improve the overall loss performance and fairness by regulating the buffer sharing in a packet switch. A transient analysis of TSD is derived to prove the fairness of buffer allocation. Computer simulation shows that the overall loss performance of TSD approaches to the pushout (PO) scheme, which is considered as an optimal solution with implementation difficulties in high-speed Internet. However, unlike the PO, the TSD will block the unwanted packets before they enter the queue, and does not need to pre-empty the queue for accepting new packets. By rejecting the arrival packets before they enter the buffer, the TSD can avoid the searching and overwriting problems in the PO. When the TSD factor is set at 16, the TSD control is very robust for achieving low overall loss probability and fairness under different traffic conditions [13].

[7] M. Mohanapriya, IlangoKrishnamurthi in their paper entitled "Modified DSR protocol for detection and removal of selective black hole attack in MANET" proposed a light weight solution methodology which is a simple acknowledgement scheme to detect gray hole nodes in MANET. It can be incorporated with any existing AODV protocols. By the proposed algorithm, the destination node detects the presence of malicious nodes in the source route and with the help of intrusion detection system the malicious nodes are isolated from the network. In this approach IDS nodes will turn into promiscuous listening only in the presence of suspected nodes resulting less energy loss, which makes approach suitable for the resource constrained characteristics of MANET. The simulation results show that the percentage of data packet loss is better than DSR in presence of multiple gray hole nodes [14].

[8] Xiao B, Yu B in their paper entitled "Identify suspect nodes in selective forwarding attacks" proposed a scheme that randomly selects part of the intermediate nodes along a forwarding path as checkpoint nodes which are responsible for generating acknowledgments for each packet received. If suspicious behavior is detected, it will generate an alarm packet and deliver it to source node. However, the algorithm suffers from high overhead because for each received packet the intermediate nodes need to send an acknowledgment back to the source node. Moreover, the authors also assume that the channel is perfect and any packet loss is due to the presence of malicious nodes [15].

## IV. RESEARCH GAPS

- Most of the research in the past for detecting selective black hole attack has been carried out on threshold based mechanisms but a little work is done on distributed cooperative mechanism basis. 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 selective packet drop attack in AODV protocols based on statistical methods.
- Most of the work has been carried out for tackling with selective packet drop 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 selective packet drop attack in MANET has not been accounted so for according to author's knowledge.

## V. CONCLUSION

Only intrusion detection and prevention techniques are not sufficient for securing wireless network but there is also need of good Intrusion Detection System. There are many researchers who design and developed many techniques for detecting and preventing selective packet drop attacks in MANET. Some techniques are effective for improving throughput and other for delay time. But design of an efficient technique for improving both remains an open challenge. Future work will involve developing an efficient framework for detecting selective packet

drop attack in MANET and to measure its performance with parameters like throughput, delay, packet loss, end-to-end packet delivery ratio etc.

## VI. 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 2012and 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. AsriNgadi, 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]**SagarPatolia, Harmandeep Singh, "Review of Isolate and Prevent Selective Packet Drop Attack in MANET", "International Journal of Innovative Research in Science, Engineering and Technology", Vol. 3, Issue 12, December 2014 and ISSN: 2319-8753.

**[7]**SagarBabubhaiPatolia ,Narendra Kumar, "KEAM- To Isolate and Prevent Selective Packet Drop Attack in MANET", "International Journal of Innovative Research in Science, Engineering and Technology", Vol. 4, Issue 5, May 2015, ISSN(Online) : 2319 – 8753 and ISSN (Print) : 2347 – 6710.

**[8]**Archana and Maya Mohan, "An Intrusion Detection System for MANET against Selective Packet Dropping", "International Journal of Computer Applications Advanced Computing and Communication Techniques for High Performance Applications", 2014and ISSN: 0975-8887.

**[9]** Anita and Abhilasha, "A Novel Technique to Protect and Isolate Selective Packet Drop Attack in MANET", "International Journal of Advanced Research in Computer and Communication Engineering", Vol. 3, Issue 6, June 2014, ISSN (Online): 2278-1021 and ISSN (Print): 2319-5940.

**[10]** N.Bhalaji and Dr. A.Shanmugam, "Reliable Routing against Selective Packet Drop Attack in DSR based MANET", "JOURNAL OF SOFTWARE", VOL. 4, NO. 6, AUGUST 2009.

**[11]** Ming-Yang Su, "Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems", "Elsevier Journal of Computer Communications", Volume 34, Issue 1, January 2011.

**[12]** Shah Vrutik, NileshModi, PataniAshwin, "AODVGAP-An Acknowledgment based approach to mitigate selective forwarding attacks in MANET", "International journal of Computer Engineering & Technology (IJCET)", Volume 3, Issue 2, July- September (2012), ISSN 0976 – 6367(Print), ISSN 0976 – 6375(Online).

**[13]**Jui-Pin Yang, Yuan-Sun Chu, and Ming-Cheng Liang, "Threshold-Based Selective Drop for Shared Buffer Packet Switches", "IEEE Communication letters", Volume 7, Issue 4 and ISSN 1089-7798.

**[14]** M. Mohanapriya, IlangoKrishnamurthi in their paper entitled "Modified DSR protocol for detection and removal of selective black hole attack in MANET", "Journal of Computers and Electrical Engineering", Vol. 40, Issue 2, February, 2014 and ISSN: 0045-7906.

**[15]** Xiao B, Yu B, Gao C, "CHEMAS: identify suspect nodes in selective forwarding attacks", "Journal of Parallel Distributed Computing", 2007and ISSN 1218-1230.

**[16]**Jaehak Yu, Hansung Lee, Myung-Sup Kim , Daihee Park, "Traffic flooding attack detection with SNMP MIB using SVM", "Elsevier Journal of Computer Communications", Volume 31, September 2008.

**[17]** D. Cerri, A. Ghioni, "SecuringAODV: The A-SAODV Secure Routing Prototype", "IEEE Communication Magazine", Feb. 2008, pp 120-125.

**[18]** K. Mishra, B. D. Sahoo, "A Modified Adaptive-Saodv Prototype For Performance Enhancement In Manet", "International Journal Of Computer Applications In Engineering, Technology and Sciences", Apr. 2009 – Sep. 2009, pp 443-447.

**[19]** Ming-Yang Su., "A study of deploying intrusion detection systems in

**[20]**Munish Sharma and Anuradha, "Network Intrusion Detection System for Denial of Service Attack based on Misuse Detection", "IJCEM International Journal of Computational Engineering & Management", Vol. 12, April 2011 ISSN (Online): 2230-7893.