ISSN: 2995-3286

Research Article

International Journal of Media and Networks

Finding Packet Dropper and Collecting Missing Packet due to Packet Dropping Attackers in Mobile Adhoc Network Using Divide and Conquer Algorithm

S. Hemalatha[1*], Harikumar Pallathadka[2] and Rajesh P Chinchewadi[3]

[1]*Post-Doctoral Research Fellow, Manipur International University, Imphal , Manipur, India*

[2]*Vice Chancellor and Professor, Manipur International University, Imphal, Manipur, India*

[3]*CTO& amp; Dean Innovation, Manipur International University, Imphal, Manipur, India.*

[*]Corresponding Author
S. Hemalatha, Post-Doctoral Research Fellow, Manipur International University, Imphal , Manipur, India.

Submitted: 2023, Dec 04 **Accepted:** 2023, Dec 26 **Published:** 2024, Jan 05

Citation: Hemalatha, S., Pallathadka, H., Chinchewadi, R. P. (2024). Finding Packet Dropper and Collecting Missing Packet due to Packet Dropping Attackers in Mobile Adhoc Network Using Divide and Conquer Algorithm. *Int J Med Net, 2*(1), 01-06.

Abstract

Objective: *Finding the Packet dropping attacker and collecting the missing packet in the MANET is one of the challenging task since the characteristics of the MANET node mobility. Packet Transmission from the source node to the Destination node is done after sending the Route Request and Route Reply, reliable path chosen based on the protocol selection in Mobile Adhoc Network which is self-organized running without any basic infrastructure. Data which is going to send by the sender is divided in to the packet and put sequence numbering on the packet finally transmitted on the medium. Each and every packet get travelled on the assigned path to reach to the destination. If any packet missed on the transmission the source node has to retransmit to the destination. while forwarding the packet from one hop to another the packet dropper attacks are play dropping the packets.*

Methods: *There are several methods were proposed for elaborating the packet dropping attacks and solution for finding the attackers in the MANET, but none of the methods proposed for collecting the missed packet instead of getting retransmission. Divide and conquer method between the route to destination path applied to finding the packet dropper attacker and collecting the missing packet from the previous node.*

Findings: *The proposed method could be implement using network simulator and performance result could be better than existing packet dropper attacker work.*

Novelty: *This proposed article shows packet dropper attackers in the MANET and collecting the missing packet by using the divide and conquer algorithm in the source to destination path route.*

Keywords: MANET, Missing Packet, Divide and Conquer Algorithm, Packet Dropper Attack.

1. Introduction

Mobile Adhoc Network (MANET) is a self-organizing communication network with the support of collection of wireless nodes in the objective of making communication via message forwarding [1]. Due to the limitation and design challenges of MANET this network could able to create and support for the instant communication application development for communication like military, disaster management , emergency services [2]. While making communication among the nodes the packet may leads to fails on reaching to the destination node due to internal nodes parameter lags like power failure, nodes mobility ,insufficient buffer space and external attackers like DDoS attacks finally all these factors affects the overall performance of the MANET throughput and other factors [3,4]. Packet drops due to system failure is neglected where as other factors various mechanism proposed to overcome the packet drop problems but still the new attacks are forming for packet dropping attacks and research are continuing to overcome the new attacks, all these because of lack of physical protection mechanism and reliable medium access mechanism in routing functions in MANET [5-7].

All the categories of packet dropping and attacks in MANET with the proposed solution with respect to the internal factor and external security attacks forces. Internal factors are natural happen could able to prevent and make the alternate solution from the packet drop whereas external factors are difficult to compute and need a method to detect and avoid. Overall all classifications of packet dropping attacks and methods are shown in the Figure 1.

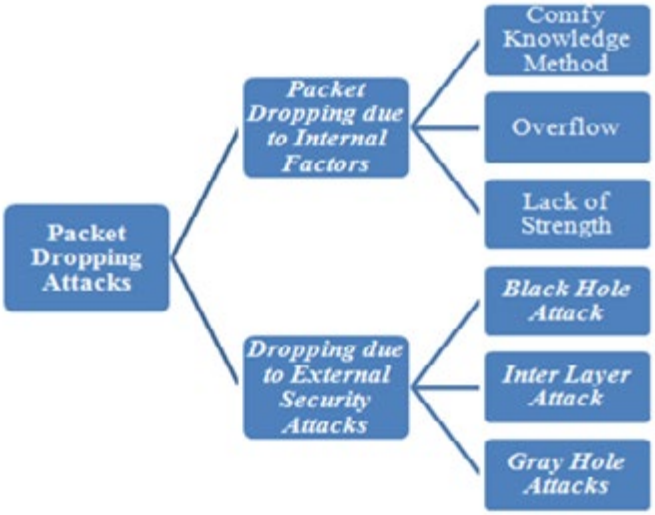

Figure 1: Packet Dropping Attacks and Methods

Packet Dropping Due to Internal Factors

One of the available algorithm to monitor the dropping of packet is called the comfy knowledge method [4] which compute the cause of packet dropping. Another methods determines the packet drop causes of overflow and lack of strength [8]. Both the methods does not prevent the packet loss or drop. But the packet drop due to buffer over flow could be detect by using Random Early Detection (RED) with computing the number packet in the queue using the RED Equation as follows in the equation (1) can be used for selecting the nodes for packet transmission which has lease Q Average value.

$Q_{average}$ = Weighted Constant *Instant_Packet_Queued+(1 - Weighted Constant) * Average Packet Old Queue. ----------Equ (1)

Packet dropping is due to lack of energy in the MANET nodes , can be computed by maintaining the Packet Handling Ability of individual nodes, which can be done using the following equation (2), nodes which are having more PHA can be selected for route selection node.

PHA = Residual energy of the node / Energy required by node to forward the packet

--------Equ (2)

In Black hole attack Malicious node is launched in the MANET, which creates the attacks on the network packets by not forwarding the selective packets to the next hope from number of packets received [6]. In ***Gray hole attacks,*** Malicious node is launched in the MANET, those nodes hold the selective one packet which never forward to the next hope from the n number of packets on the window [9]. This two protocols attacks are difficult to detect since the malicious nodes are intrude in to the network and make trustworthy to the neighbouring nodes, suddenly falls on doing the attacking roles without any alarm. Ultimate aim of this attackers is to reduce the MANET performance. Whereas ***Inter Layer Attack,*** the malicious node delayed the respond of the RTS and CTS messages to the sender which causes the sender node assumes medium is not free for transmission, after a long trail of RTS the sender nodes realises that malicious node in the MANET. ***Watchdog and Pathrater*** is a kind of intruder detection system, it checks all the nodes behaviour by monitoring the packets forwarding , any nodes fails to forward the packet to the next hope a certain threshold is maintain which exist the threshold limit then the watchdog intimate to the sender about the malicious nodes activities, also the pathrater will support the sender to avoid malicious node route path is selected for transmission [10-12].

There are two categories of solution is given for thwart packet dropping attacks in MANET for improving the TCP layer performance [13]. (1)Credit based Systems and (2) Reputation based Systems .Apart from that two techniques the traditional End to end scheme also support for thwart the Packet dropping attacks. The classification of different technique is depicted in the Figure 2.

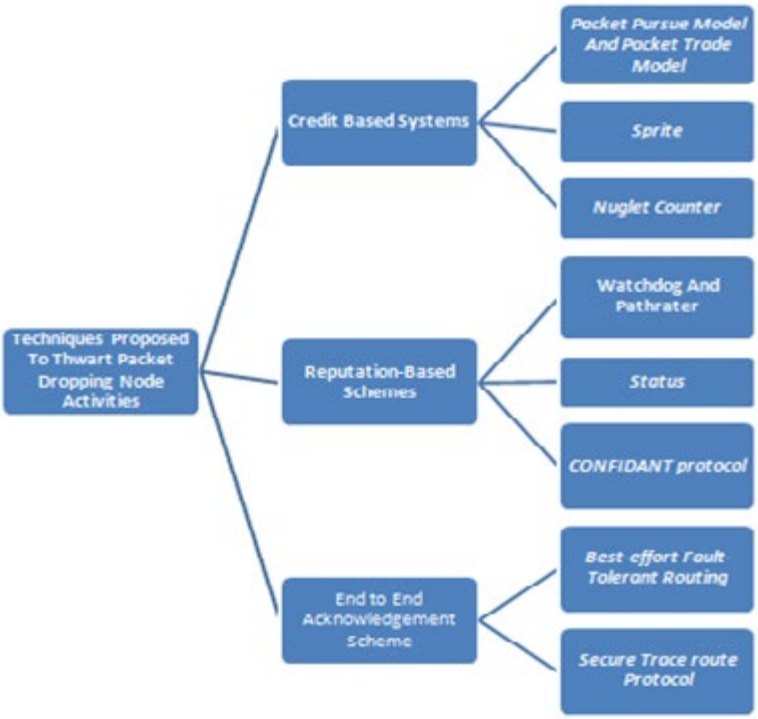

Figure 2: Techniques Proposed to Thwart Packet Dropping Node Activities

In the credit based systems incorporates packet pursue model and Packet trade model which uses a nuggets concept [14]. The sender add some nuggets on the sending packets, intermediate modes collects the certain amount of nuggets when it forward the packet to the next hop as well send the forwarded messages to the sender nodes. When a packets get dropped by the intermediate node called packet dropper then the Packet trade model trade the packet from it buffer by collecting the nuggets. Nuglet Counter technique a nuglet counter is maintained in every node , when a packet send from the sender the counter decreases and when a packet forward by the node the counter increases ,this counter increasing and decreasing MANET uses Tamper- resistant hardware modules [15]. A special Network architecture with a Credit Clearance Service (CCS) In MANET [16]. All the nodes capable of receive the receipt of received and forwarded services with the support of CCS. When a node receive a packet it receives CCS receipt and forward the packet it receives the forwarded receipt. This mechanism support for finding the packet dropping nodes.

All these above discussed technique uses the some external devices and software support for finding the packet dropper nodes. Watchdog and Pathrater It is a kind of intruder detection system it checks all the nodes behaviour by monitoring the packets forwarding, any nodes fails to forward the packet to the next hope a certain threshold is maintain which exist the threshold limit then the watchdog intimate to the sender about the malicious nodes activities, also the pathrater will support the sender to avoid malicious node route path is selected for transmission. CONFIDANT protocol has four modules called the Monitor, the Reputation System, the Path Manager, and the Trust Manager proposed by, all the nodes continuously monitoring the first hope neighbour with functions of neighbour node surveillance, node ranking, path evaluation, and sending and receiving alarm messages [17-21]. Any misbehaviours find on the function the nodes alarms to the trust manager about the malicious nodes. Status uses a data structure status about each node maintains in all other nodes , this information is broadcast to all other nodes periodically along with the credit count.

In the TCP protocol End to end acknowledgment scheme is employed in MANET protocol stack [22-24]. When a sender sends the packet with the sequence numbering on the packet parallel the receiver replies the acknowledgments (ACK) in a continuous stream of packet receiving otherwise receiver send the selective Acknowledgment (SACK). Another kind of ACK is called 2ACK technique which used to find out the miscellaneous nodes who committed the forwarding of packet but not forwarding. Secure Trace route Protocol proposed by , to find out malicious nodes by setting the Time-To Live (TTL) to the packets, when the TTL expires the receives a warning messages from the router to the nodes where the TTL expires. Best-effort Fault-Tolerant Routing (BFTR) proposed by, this scheme monitors continuously about the quality of the path used also compared with the previous path quality, if any variation degrades the path quality alert the network about the malicious path chosen [25,26].

From the different technique followed for thwart the Packet dropping attacks are still needs progress to find the solution for new kind of attacks. Instead of finding the packet dropping malicious node, collecting the missing packet from the routing path node can give the better solution for TCP Performance improvement. There is a need of maintaining virtual buffering in all the intermediate nodes to store about the forwarding packets as well as an Artificial Intelligence technique is needed to collect

the missing packets.

In this article proposed the new method called Missing packet transmission algorithm for not only identifying the packet dropper attacker also collect the missing packet using the divide and conquer strategy. The destination node send a special request message to the middle node to resend the missing packet using the divide and conquer strategy recursively apply the mechanism could collect the missing packet as well as identifying the packet dropper attacker.

The remainder of this paper will discuss the methods that presented the missing packet detection algorithm in section 2. Section 3 results and discussion elaborates how to carried out the research with the Network simulator together with the help of MANET parameters to locate the comparison study, and Section 4 concludes the research job.

2. Methodology

Divide and Conquer technique is the one of the best mathematical technique to solve the any problematic issues, this missing packet assembly will be done it in the receiver end , whenever the packet is missed in the MANET , the solution given is resending of packet from the source to the destination . The proposed algorithm uses a technique is called divide and conquer which divide the route in to two half, the middle node is responsible for retransmitting the missing packet to the destination .The details working of this algorithm shown in the Algorithm3.1.

Algorithm 1 Missing Packet Transmission Algorithm Consist of Following Stage

Stage 1: Find a path from source node S to the destination node D by sending the route request and Route reply

Stage 2: Set the Middle node

(i) fine number of Hop from source to the destination

(ii) Middle node = Number of hop / 2

Stage 3: Transmit the Packet from source to destination

Stage 4: From the Destination any packet receiving is missed

(i) Destination node send Retransmission of missed packet number to the middle node

if Middle node is not retransmit the packet

store the middle node

Find a new middle from the source node to the middle

go to stage 4

Stage 5: All the recessive middle node are not finding the retransmission , source node retransmit the packet gain.

Stage 6: Find the Packet dropper attacker

Label Check

If the Middle node is not forward the missing packet then the attacker from source to middle

Repeat the process and find the new middle node go to label check

else

Send the latest middle node as a packet dropper attacker

3. Result and Discussion

To analysis the MANET proposed work , the result of simulator work need to evaluate with some metric.

Throughput

Its defined as total number of packets reaches at the destination node in a time interval. In MANET the throughput can be affected by frequent topological changes, power factor, unreliable communication between the node , etc

Throughput = Total Packet size / Transmission time

where transmission time = Total Packet size / bandwidth

Packet Delivery Ratio

It is defined as that ration between total number of packet delivered at destination node and total number of packet.

Packet Delivery Ratio = Total Packet delivered at destination / Total number of

Packet generated by the source

Route Overhead

The total number of route transmission generated for RREQ, RREP, RERR , from route protocol.

Route Overhead = Number of RTR packet

End to End Delay

Average time taken for sending packet from source to the destination. The delay due to delay in route discovery, packet in Queue, latency, wireless link etc.

Packet Loss Ratio

Total number of packet not reached to the destination it is opposite to the packet delivery ratio.

Network Load

The average number of packet carried by entire network.

Simulation Parameter Setup

The following simulator parameter value has to use for NS2 simulation result carried out

Parameter

Network Area

Network area can be set any range from 200X 200 to 2500X 2500 range in m2

Simulation time

Simulation time can be set by varying 5 s to 3600 s

Mobility speed

Mobility speed could be 5ms to 50 ms

Number of Network nodes

Total number of MANET node from 50 to 600 nodes

Number of packet dropping attacker node

total number of dropping attacker node from 6 to 60

Packet Rate

Packet transmission rate varies from 1 packet to 25 packet per second

4. Conclusion

This article elaborated divide and conquer strategy applied to the MANET packet travelling route path from the source node to the destination node which support for finding packet dropper attacker and collecting the missing packet due to packet dropping attackers in MANET also alert the packet dropper attacker in the MANET. This can be implemented using any network simulator and compare with the existing method to find out the performance.

References

1. Samreen, S. (2021). Shielding against on-off attack pattern in a MANET through a trust computation scheme leveraging the behavioural consistency. International Journal of Communication Networks and Distributed Systems, 27(2), 178-213.
2. Samreen, S., & Meerja, A. J. (2018). Improved recommendation filtering component resilient to trust distortion attacks in a MANET. In Smart Secure Systems–IoT and Analytics Perspective: Second International Conference on Intelligent Information Technologies. ICIIT 2017, Chennai, India, December 20-22, 2017, Proceedings 2 (pp. 81-92). Springer Singapore.
3. Kampitaki, D. G., & Economides, A. A. (2023). Selfishness in Mobile Ad-Hoc Networks: A Literature Review on Detection Techniques and Prevention Mechanisms. IEEE Access.
4. Joardar, S., Sinhababu, N., Dey, S., & Choudhury, P. (2023). Mitigating DoS attack in MANETs considering node reputation with AI. Journal of Network and Systems Management, 31(3), 1-34.
5. Hussain, M. A., & Duraisamy, B. (2020). Preventing Malicious Packet Drops in MANETs by Counter Based Authenticated Acknowledgement. Ingénierie des Systèmes d'Information, 25(2).
6. Kanthimathi, S., & Jhansi Rani, P. (2022). An efficient packet dropping attack detection mechanism in wireless ad-hoc networks using ECC based AODV-ACO protocol. Wireless Networks, 1-13.
7. Vijayalakshmi, S., Bose, S., Logeswari, G., & Anitha, T. (2023). Hybrid defense mechanism against malicious packet dropping attack for MANET using game theory. Cyber security and applications, 1, 100011.
8. Narayana, V. L., & Bharathi, C. R. (2023). Efficient route discovery method in MANETs and packet loss reduction mechanisms. International Journal of Advanced Intelligence Paradigms, 25(1-2), 129-140.
9. Mankotia, V., Sunkaria, R. K., & Gurung, S. (2023). DT-AODV: A dynamic threshold protocol against black-hole attack in MANET. Sādhanā, 48(4), 190.
10. Reddy, V., Mohammad, A. A. K., Rajani, D., Maddumala, V. R., & Veeravasantharao, B. (2023). Mitigating Packet Dropping Nodes from MANETs due to System faults.
11. Ambika, I., Bhatia, S., Basheer, S., & Dadheech, P. (2023). Optimized Resource Allocation and Queue Management for Traffic Control in MANET. Computer Systems Science & Engineering, 45(2).
12. Shukla, D., & Singh, R. (2023, March). Performance Assessment of DSDV and AODV Routing Algorithms in MANET under Active Black Hole Assault. In 2023 6th International Conference on Information Systems and Computer Networks (ISCON) (pp. 1-6). IEEE.
13. Alabady, S. A., & Hameed, A. N. (2023). Design, Simulation, and Performance Evaluation of Reactive and Proactive Ad-Hoc Routing Protocols.
14. Olanrewaju, O. M., Abdulwasiu, A. A. A., & Nuhu, A. (2023). Enhanced On-demand Distance Vector Routing Protocol to prevent Blackhole Attack in MANET. International Journal of Software Engineering and Computer Systems, 9(1), 68-75.
15. SARKAR, S. K., GHOSH, J., BISWAS, R., & FAIZAN, M. (2023). An Investigation on Routing Techniques and Devolopment of a Secured Routing Techniques for Improving Performance and Security of Manets.
16. Kaddoura, S., Haraty, R. A., Al Jahdali, S., & Assi, M. (2023). SDODV: A smart and adaptive on-demand distance vector routing protocol for MANETs. Peer-to-Peer Networking and Applications, 16(5), 2325-2348.
17. Segara, A. J. T., & Ramadhani, A. D. (2023). Performance Analysis of Mobile Ad-Hoc Networks Based on TCP and UDP Traffic on AODV Protocol for Warship Communication. Journal of Systems Engineering and Information Technology (JOSEIT), 2(2), 53-58.
18. Susanto, B. M., Hariyanto, A., & Surateno, S. (2018). Performance Comparison of Proactive and Reactive Routing Protocol in Mobile Ad Hoc Network. Journal of Communications, 13(5), 218-224.
19. Alabdullah, M. G. K., Atiyah, B. M., Khalaf, K. S., & Yadgar, S. H. (2019). Analysis and simulation of three MANET routing protocols: A research on AODV, DSR & DSDV characteristics and their performance evaluation. Periodicals of Engineering and Natural Sciences, 7(3), 1228-1238.
20. AL-Dhief, F. T., Sabri, N., Salim, M. S., Fouad, S., & Aljunid, S. A. (2018). MANET routing protocols evaluation: AODV, DSR and DSDV perspective. In MATEC web of conferences (Vol. 150, p. 06024). EDP Sciences.
21. Sadakale, R., Patil, R. A., & Ramesh, N. V. K. (2019). An efficient AODV routing protocol for vehicular Ad hoc network. Int. J. Innov. Technol. Explor. Eng, 8(4), 1-4.
22. Nasional, T. Riset, I. P. Series, and S. Vol, (2020) "Performansi Protokol Routing Aomdv, Dsr, Dan Aodv Pada Mobile Ad-Hoc Network (Manet)," Eng. Sci., vol. 6, no. 1, pp. 887–894, 2020.
23. Mohammad, A. A. K., Mahmood, A. M., & Vemuru, S. (2019). Intentional and unintentional misbehaving node detection and prevention in mobile ad hoc network. International Journal of Hybrid Intelligence, 1(2-3), 239-267.
24. Sakthivel, T., & Chandrasekaran, R. M. (2018). A dummy packet-based hybrid security framework for mitigating routing misbehavior in multi-hop wireless networks. Wireless Personal Communications, 101(3), 1581-1618.
25. Govindaraj, L., Sundan, B., & Thangasamy, A. (2021, December). An intrusion detection and prevention system for ddos attacks using a 2-player bayesian game theoretic

approach. In 2021 4th International Conference on Computing and Communications Technologies (ICCCT) (pp. 319-324). IEEE.
26. Thangasamy, A., Sundan, B., & Govindaraj, L. (2021, December). Dynamic phad/ahad analysis for network intrusion detection and prevention system for cloud environment. In 2021 4th International Conference on Computing and Communications Technologies (ICCCT) (pp. 273-279). IEEE.