ISSN: 2995-3286

Research Article

International Journal of Media and Networks

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). 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), 01-05.

Abstract

In a mobile ad hoc network, packet transmission is essential to prevent packet drops along the transmission path. Attackers who drop forwarded packets are present in the MANET and are attempting to lower the MANET's performance. There are several ways to identify packet dropper attackers and warn the MANET about them. The divide and conquer tactic is used in this research study to identify the attacker who dropped the packets and to obtain the missing packet from the intermediary source. This task will be accomplished by adding an extra buffer to hold the forwarded packet during its whole round trip from source to destination. The findings of the suggested work's implementation using the network simulator and comparisons with those of the current methodology ultimately demonstrate that the divide and conquer approach has demonstrated the MANET's performance.

Keywords: MANET, Missing Packet, Divide and Conquer Algorithm. Post-Doctoral Research Fellow, Manipur International University, Imphal , Manipur, India.

1. Introduction

Mobile Adhoc Network (MANET) is a self-organizing communication 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]. This network nodes can able to send and receive the communication packets across the communication range. Network layer in the MANET protocol stack plays the major role for communication across the nodes. Communication messages can divided in to packets, packets are forms a sequence number , the same order the packet can travel from source node to the destination nodes via several intermediate nodes which are discovered in the route discovery stages with the support of Route Request and Route Reply messages.

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. 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 [3].

Even though the Transport layer protocols in the MANET like TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) which support end to end communication link between the source node to destination nodes could not able to detect the packet dropper nodes with the support of ACK (Acknowledgement) Message. Research on Security in MANET needed in data transmission as well as route discovery . The Packet can be drop at MAC layer or Network layer. In MAC layer due to the packet transmission buffer size , the packet from the higher layer will be dropped if the buffer is full called buffer overflow. The solution is for buffer flow is retransmission of Packet as per the IEEE 802.11 Protocol specification with the support of Request to Send . Another reason of packet loss in Physical layer is hidden and Exposed terminal problem, high bit rate transmission , interference while radio transmission. Apart from that selfish nodes are with the intend to maintain the nodes battery power could not participating the forwarding the packet to the next hope. due to all the reasons still the analysing of packet dropping is a challenges in MANET need a solution to improve the MANET protocol stack.

This remaining of this article is planned to provide the packet dropper attacks and survey in the following section 2, different techniques proposed to thwart packet dropping node activities in MANET in section 3 and Conclusion in section 4.

p dropping and packet dropping attacks related survey
In this section elaborate the 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 2.1

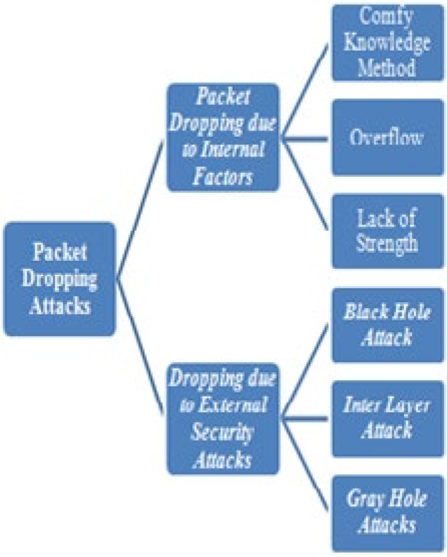

Figure 2.1: Packet Dropping Attacks and Methods

2.1 Packet Dropping Due to Internal Factors

One of the available algorithm to monitor the dropping of packet is called The comfy knowledge method which compute the cause of packet dropping [4]. Another methods determines the packet drop causes of overflow and lack of strength [5]. 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

2.2.Packet Dropping Due to External Security Attacks Forces

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].

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 [7].

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.

Inter Layer Attack

The default MAC protocol IEEE configuration is modifies by the malicious node , for instant 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.

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

2.2.1 Developed Solution for External Security Forces

Watchdog and Pathrater

Watchdog and Pathrater [8]. 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.

Methodology

Techniques Proposed To Thwart Packet Dropping Node Activities in MANET

Since the Packet dropping is not only affect the MAC layer, Network layer which also affects the TCP layer performance factors. There are two categories of solution is given for thwart packet dropping attacks in MANET for improving the TCP layer performance. (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 Figure3.1 .

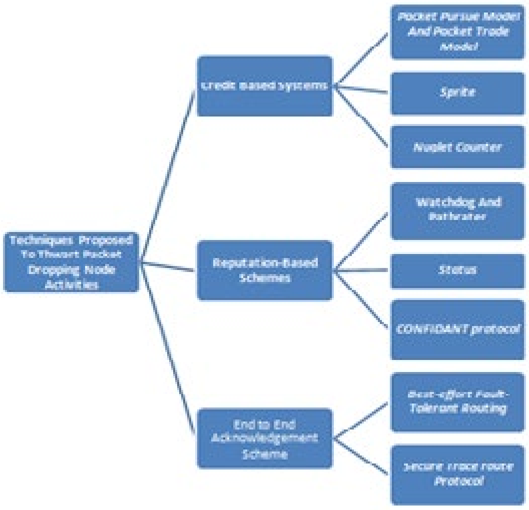
Techniques Proposed To Thwart Packet Dropping Node Activities
Credit Based Systems
Reputation-Based Schemes
End to End Acknowledgement Scheme
Packet Pursue Model And Packet Trade Model
Sprite
Nuglet Counter
Watchdog And Pathrater
Status
CONFIDANT protocol
Best-effort Fault-Tolerant Routing
Secure trace route Protocol

Figure 3.1: Techniques Proposed To Thwart Packet Dropping Node Activities

3.1 Credit Based Systems

Packet Pursue Model and Packet Trade Model

In the credit based systems incorporates packet pursue model and Packet trade model [9] which uses a nuggets concept. 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

In this 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 [10].

A special Network architecture with a Credit Clearance Service (CCS) In MANET [11]. 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.

3.2 Reputation-Based Schemes

In the reputation based schemes the malicious node can be detect and declare.

Watchdog and Pathrater

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 [8].

CONFIDANT Protocol

This protocol has four modules called the Monitor, the Reputation System, the Path Manager, and the Trust Manager proposed by Buchegger and Le Boudec, 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. Any misbehaviours find on the function the nodes alarms to the trust manager about the malicious nodes [12].

Status

In this technique 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 [13].

3.3: End to End Acknowledgement Scheme

In the TCP protocol End to end acknowledgment scheme is employed in MANET protocol stack. 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

Secure Trace route Protocol proposed by Padmanabhan and Simon, 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 [14].

Best-effort Fault-Tolerant Routing

Best-effort Fault-Tolerant Routing (BFTR) proposed by Xue and Nahrstedt, 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 [15].

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 a Artificial Intelligence technique is needed to collect the missing packets.

Divide and Conquer Mathematical Background

divide and Conquer is a one of the mathematical solution for a complex problem, which has three parts divide conquer and combine . divide parts divide the problem in to smaller parts as possible, Conquer solve each sub problems recursively, and combine join all the solved problem to get the final solution. In a MANET this divide and conquer is applied to the route path from the source to the destination. The number hops determines the travels of the packet from source node to the destination node.

Divide: Divide the number of hop from source to destination in to two half again each half divide in to two recursively as much as possible .

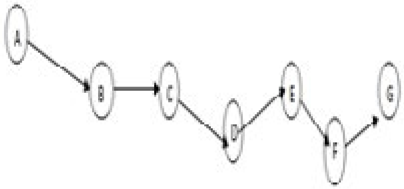

Figure 4.1: Route Path From Source to the Destination Node

A - Source Node
G -Destination Node
Total number of hop 6
first middle = 6/2 = 3 = D node
Second Middle = 3/2 = 1 or 2 = B or C node

Conquer: Destination node send the missing packet request to the first middle node. If the destination received the packet , then problem solved otherwise send the request for second middle node recursively until the packet received

Combined: In this stage is combined the middle node status.

Proposed methods for dropped packet assemble using divide and conquer technique.

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 Algorithm 3.1.

Algorithm 4.1 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
```

5. Conclusion

The proposed divide and conquer algorithm for collection the missing packet due to packet dropping attackers in MANET also finding out 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. Giordano, S. (2002). Mobile ad hoc networks. Handbook of wireless networks and mobile computing, 325-346.
2. Bang, Ankur O., and Prabhakar L. Ramteke. (2013) "MANET: History, challenges and applications." International Journal of Application or Innovation in Engineering & Management (IJAIEM) 2.9 (2013): 249-251.
3. 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.
4. Siddiqua, A., Sridevi, K., & Mohammed, A. A. K. (2015, January). Preventing black hole attacks in MANETs using secure knowledge algorithm. In 2015 International Conference on Signal Processing and Communication Engineering Systems (pp. 421-425). IEEE.
5. Mohammad, A. A. K., Mirza, A., & Vemuru, S. (2016). Analytical Model for Evaluating the Bottleneck Node in MANETs. Indian Journal of Science and Technology, 9, 31.
6. Al-Shurman, M., Yoo, S. M., & Park, S. (2004, April). Black hole attack in mobile ad hoc networks. In Proceedings of the 42nd annual Southeast regional conference (pp. 96-97).
7. Yu, W. (2005). Defense against routing disruptions in mobile ad hoc networks. IEEE INFOCM 2005, Mar.
8. Marti, S., Giuli, T. J., Lai, K., & Baker, M. (2000, August). Mitigating routing misbehavior in mobile ad hoc networks. In Proceedings of the 6th annual international conference on Mobile computing and networking (pp. 255-265).
9. Buttyan, L., & Hubaux, J. P. (2000, August). Enforcing service availability in mobile ad-hoc WANs. In 2000 First Annual Workshop on Mobile and Ad Hoc Networking and Computing. MobiHOC (Cat. No. 00EX444) (pp. 87-96). IEEE.
10. Buttyán, L., & Hubaux, J. P. (2003). Stimulating cooperation in self-organizing mobile ad hoc networks. Mobile Networks and Applications, 8, 579-592.
11. Zhong, S., Chen, J., & Yang, Y. R. (2003, March). Sprite: A simple, cheat-proof, credit-based system for mobile ad-hoc networks. In IEEE INFOCOM 2003. Twenty-second Annual Joint Conference of the IEEE Computer and Communications Societies (IEEE Cat. No. 03CH37428) (Vol. 3, pp. 1987-1997). IEEE.
12. Buchegger, S., & Le Boudec, J. Y. (2002, June). Performance analysis of the CONFIDANT protocol. In Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing (pp. 226-236).
13. Miranda, H., & Rodrigues, L. (2002, October). Preventing selfishness in open mobile ad hoc networks. In Proc. Seventh CaberNet Radicals Workshop.
14. Padmanabhan, V. N., & Simon, D. R. (2003). Secure traceroute to detect faulty or malicious routing. ACM SIGCOMM Computer Communication Review, 33(1), 77-82.
15. Xue, Y., & Nahrstedt, K. (2004). Providing fault-tolerant ad hoc routing service in adversarial environments. Wireless Personal Communications, 29, 367-388.