International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7255
***Article Received**: 20 April 2023 **Revised:** 21 June 2023 **Accepted:** 09 July 2023*

Challenges on Missing Packet Detection or Packet Dropping Attacks in Mobile Adhoc Network -A Survey

Dr. S. Hemalatha[1], Dr. Harikumar Pallathadka[2], Prof Rajesh P Chinhewadi[3], Dr. D. Kalaiyarasi[4], Dr. B. Anni Princy[5]
[1]Corresponding Author, Professor/ Department of Computer Science and Business System,
Panimalar Engineering College,
Chennai, Tamil Nadu, India
pithemalatha@gmail.com
Post Doctorial Research Fellow,
Manipur International University,
Imphal ,Manipur, India
[2]PhD, DSc, Vice Chancellor and Professor, Manipur International University, Imphal , Manipur, India
harikumar@miu.edu.in
[3]CTO& Dean Innovation, Manipur International University, Imphal ,Manipur, India
Rajesh.cto@miu.edu.in
[4]Professor ,Department of Electronic and Communication Engineering, Panimalar Engineering College, Chennai, Tamil Nadu India
kalaiccarthi@gmail.com
[5]Professor, Computer and Communication Engineering, Panimalar Engineering College, Chennai ,Tamilnadu , INDIA
ccehod@panimalar.ac.in

Abstract—Collection of wireless nodes forms together to communicate each other in the network without infrastructure less and any access point along with the characteristics of freedom in mobility is called Mobile Adhoc Network. Transmitting of packets from source to destination plays the vital role in MANET. When a Packet is not delivered properly at the destination , its affects the performance of the MANET. Due to this characteristics of the mobility nodes can subject to falls on the packet missing also the various packets dropping security attacks take part in the dropping the packets while communication to achieve the decreasing the performance of the MANET. This article focus on the survey about the missing packet assembly as well the packet dropping security attacks in MANET.

Keywords- MANET, Packet, Security ,Packet drop, Fragmentation and Assembly.

I. INTRODUCTION

Mobile Adhoc Network (MANET) is a self organizing communication network [1] with the support of collection of wireless nodes in the objective of making communication via message forwarding. Due to the limitation [2] 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. 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 [3] 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.

Even though the Transport layer protocols in the MANET like TCP (Transmission Control Protocol) and UDP

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7255
***Article Received**: 20 April 2023 **Revised:** 21 June 2023 **Accepted:** 09 July 2023*

(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 Article is planned to elaborate the different packet dropper attacker in MANET which make a path to identify the new method for finding out packet dropper attacker. So the 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.

II. PACKET 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 where as 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

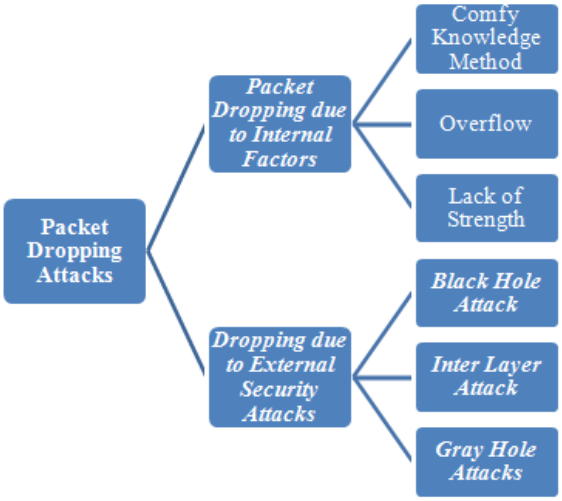

Figure 2.1 Packet Dropping attacks and methods

A. 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 [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 -------- Equ (2)

B..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].

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7255
***Article Received**: 20 April 2023 **Revised:** 21 June 2023 **Accepted:** 09 July 2023*

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.

C. 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.

III. 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 .

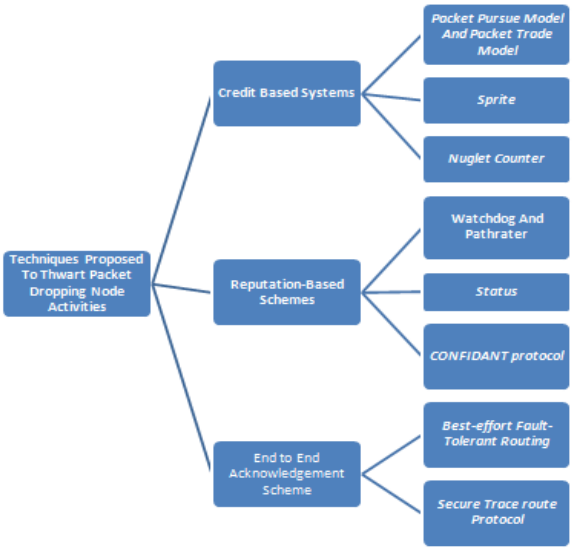

Figure 3.1 Classification of Packet Dropping Node

A.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[10] 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.

Sprite

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

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7255
***Article Received**: 20 April 2023 **Revised:** 21 June 2023 **Accepted:** 09 July 2023*

B. Reputation-Based Schemes

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

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.

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 [12], 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.

Status

In this technique uses a data structure [13] status about each node maintains in all other nodes , this information is broadcast to all other nodes periodically along with the credit count .

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 [14], to find out malicious nodes by setting the Time-ToLive (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

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

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.

IV CONCLUSION

In this survey article focuses on the packet dropping attacks and collecting the missing packet from the source . All the above discussed attack and techniques are given only prevention and detection of the packet dropping, none of the technique is given to collect the only missing packet from the sequence of packet so that retransmission of whole the sequence of packets could be avoid. This can be implement with the support of any virtual buffering concepts about maintaining the packet storage among the MANET route path nodes. Also any artificial intelligence monitoring technique can support for collecting only missing packets from the intermediate route instead of retransmission from the source.

REFERENCES

[1] Giordano, Silvia.(2002) "Mobile ad hoc networks." Handbook of wireless networks and mobile computing (2002): 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, Arshad Ahmad Khan, Ali Mirza Mahmood, and Srikanth Vemuru. (2019)"Intentional and unintentional misbehaving node detection and prevention in mobile adhoc network." International Journal of Hybrid Intelligence 1.2-3 (2019): 239-267.

[4] Siddiqua, Ayesha, Kotari Sridevi, and Arshad Ahmad Khan Mohammed. (2015)"Preventing black hole attacks in MANETs using secure knowledge algorithm." 2015 International Conference on Signal Processing and Communication Engineering Systems. IEEE, 2015.

[5] Mohammad, Arshad Ahmad Khan, Ali Mirza, and Srikanth Vemuru.(2016) "Analytical Model for Evaluating the Bottleneck Node in MANETs." Indian Journal of Science and Technology 9 (2016):

[6] Krishnan, V. G. ., Saradhi, M. V. V. ., Dhanalakshmi, G. ., Somu, C. S. ., & Theresa, W. G. . (2023). Design of M3FCM based Convolutional Neural Network for Prediction of Wheat Disease. International Journal of

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 8s
DOI: https://doi.org/10.17762/ijritcc.v11i8s.7255
***Article Received**: 20 April 2023 **Revised:** 21 June 2023 **Accepted:** 09 July 2023*

Intelligent Systems and Applications in Engineering, 11(2s), 203 –. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/2523

[7] M. Al-Shurman, S. M. Yoo and S. Park,(2004) Black Hole Attack in Mobile Ad Hoc Networks, In Proc. of the 42nd Annual Southeast Regional Conference (ACMSE'04), Huntsville, ALabama, USA, April 2004.

[8] Qureshi, D. I. ., & Patil, M. S. S. . (2022). Secure Sensor Node-Based Fusion by Authentication Protocol Using Internet of Things and Rfid. Research Journal of Computer Systems and Engineering, 3(1), 48–55. Retrieved from https://technicaljournals.org/RJCSE/index.php/journal/article/view/41

[9] W. Yu, Y. Sun and K. R. Liu,(2005) HADOF: Defense Against Routing Disruptions in Mobile Ad Hoc Networks, In Proc. of the 24th IEEE INFOCOM, Miami, USA, March 2005.

[10] Marti, T. Giuli, K. Lai,and M. Baker,(2000) Mitigating Routing Misbehavior in Mobile Ad Hoc Networks, Proc. MobiCom, Aug. 2000.

[11] L. Buttyan and J.-P. Hubaux, (2000)Enforcing Service Availability in Mobile Ad-Hoc WANs,‖ Proc. MobiHoc, Aug. 2000 .

[12] L. Buttyan and J.-P. Hubaux, (2003) Stimulating Cooperation in Self- Organizing Mobile Ad Hoc Networks,‖ ACM/Kluwer Mobile Networks and Applications, vol. 8, no. 5, 2003.

[13] S. Zhong, J. Chen, and Y.R. Yang, (2003)Sprite: A Simple, Cheat-Proof, Credit-Based System for Mobile Ad-Hoc Networks,‖ Proc. INFOCOM, Mar.-Apr. 2003.

[14] S. Buchegger and J.-Y. Le Boudec, (2002)Performance Analysis of the CONFIDANT Protocol: Cooperation of Nodes, Fairness in Dynamic Ad-Hoc Networks,‖ Proc. MobiHoc, June 2002.

[15] H. Miranda and L. Rodrigues, (2002)Preventing Selfishness in Open Mobile Ad Hoc Networks,‖ Proc. Seventh CaberNet Radicals Workshop, Oct. 2002.

[16] V.-N. Padmanabhan and D.-R. Simon, (2003) Secure Traceroute to Detect Faulty or Malicious Routing, SIGCOMM Computer Comm. Rev., vol. 33, no. 1, Jan. 2003.

[17] Y. Xue and K. Nahrstedt,(2004) Providing Fault-Tolerant Ad-Hoc Routing Service in Adversarial Environments,‖ Wireless Personal Comm., vol. 29, nos. 3-4, pp. 367-388, 2004.