Combating Resource Consumption and Byzantine Attacks in MANET through Enhanced CBDS Technique

¹Muskan Sharma, ²Chander Prabha

¹M.Tech., ²Assistant Professor (CSE) & Head, IT Department
Swami Devi Dyal Institute of Engineering & Technology, INDIA

Abstract: MANET is a network where mobile works as node and it is wireless, infrastructure-less network in which nodes can move freely and can change their positions also. It is wireless, so it needs more security than the wired network. We are using Enhanced CBDS technique here, so that we can save our network from Resource consumption and Byzantine attacks. Resource consumption attack can be detected by adding new security checks to the algorithms. If the battery and bandwidth usage of any node are not going as per optimised usage thresholds set. Byzantine Attack we will be detected as if acknowledgement is not received by source in desired time. Adding alarm packet in the CBDS technique is the Enhanced CBDS technique. It shows better results than the CBDS technique. Enhanced CBDS technique is better than 2 ACK, BFTR and DSR on the basis of various parameters like packet delivery ratio, end to end delay, and throughput.

Keywords: MANET, MANET attacks, Security in MANET, Passive attacks in MANET, ACTIVE attacks in MANET

I. Introduction

MANET is wireless network where nodes work as routers that sends packet from one node to another node through mobiles because mobile work as node in this network. CBDS is a DSR based scheme. Here we are using CBDS technique over DSR, 2ACK, BFTR because they don't have the related mechanism about detection and response, on following perimeters: Packet delivery ration, Routing overhead, Average end to end delay, Throughput. CBDS is a new mechanism for detecting malicious nodes in MANETs under gray/collaborative black hole attacks [1].

In this scheme the address of adjacent node is used as Bait destination address to bait malicious nodes to send reply RREP message. Malicious nodes are detected using reverse tracing technique. Detected malicious node is kept in black hole list so that other nodes participating in routing of message are alerted to stop co communicate with any node in that list.

II. CBDS (Cooperative Bait Detection Scheme)

Cooperative Bait Detection Scheme decreases the dubious path information of malicious nodes and the trusted nodes (without any attack) in that malicious node reply to every RREP, instead of observing whether malicious nodes would drop packets [2]. As a result, the proportion of packet dropping was disregarded, and the malicious node of gray hole attack and black hole attack would be detected by CBDS technique.

CBDS is a comprehensive detecting attacks mechanism because in initial stage it does proactive detection and then immediately it turns into reactive response in usual period. We can still avoid the chance of black hole attack in the initial stage after adding the proactive detection portion, if the detecting mechanism just purely uses reactive response detection.

With the use of CBDS technique, we can encounter Resource consumption and Byzantine attack simulated, denial of service attack floods link to node with large volume of packets and resource consumption attack depletes & consumes node energy, bandwidth and memory by broadcasting RREQ (Route Request), RREP (Route Reply) & RRER (Route Error) packets. Earlier techniques deployed to mitigate these attacks focus prevention and detection to combat individual misbehaving nodes. This paper proposes Cooperative Bait Detection Scheme (CBDS) which deals with detection and prevention attacks to combat multiple misbehaving nodes [2].

III. Enhanced CBDS Technique

In Enhanced CBDS technique it sends alarm packets to others nodes after detecting the malicious node. So that every node knows about the defective nodes and after that they will not send or receive any packet from malicious node. Adding alarm packet in the CBDS technique is the Enhanced CBDS technique [3]. It shows better results than the CBDS technique. Following is the enhanced CBDS flow chart Fig 1 scheme:

Fig. 1. Enhanced CBDS Technique Flow Chart

IV. Performance parameters

i. Packet Delivery Ratio: This is defined as the ratio of the number of packets received at the destination and the number of packets sent by the source. Here, $pktd_i$ is the number of packets received by the destination node in the i th application, and $pkts_i$ is the number of packets sent by the source node in the i th application. The average packet delivery ratio of the application traffic n , which is denoted by PDR, is obtained as:

$$PDR = \frac{1}{n} \sum_{i=1}^n \frac{pktd_i}{pkts_i}.$$

ii. Average End-to-End Delay: This is defined as the average time taken for a packet to be transmitted from the source to the destination. The total delay of packets received by the destination node is d_i , and the number of packets received by the destination node is $pktd_i$ [4]. The average end-to-end delay of the application traffic n , which is denoted by E , is obtained as:

$$E = \frac{1}{n} \sum_{i=1}^n \frac{d_i}{pktd_i}.$$

iii. Throughput: This is defined as the total amount of data (b_i) that the destination receives them from the source divided by the time (t_i) it takes for the destination to get the final packet. The throughput is the number of bits transmitted per second. The throughput of the application traffic n , which is denoted by T , is obtained as:

$$T = \frac{1}{n} \sum_{i=1}^n \frac{b_i}{t_i}.$$

V. Results

Results of Byzantine attack & Resource consumption attacks are shown with cases like ideal case, during attack, after enhanced CBDS technique.

A. Byzantine Attack: For the detection of Byzantine Attack we will be detected as if acknowledgement is not received by source in desired time. Secondly If the number address of nodes differ from the optimal path and thirdly if Packet delivery ratio falls below a minimum threshold level and will be avoided by rerouting.

Fig. 2.a Ideal Case

Fig. 2.b During Attack

Fig. 2.c After Enhanced CBDS

a. Ideal Case: Mobile nodes are sending packets to each other so that packet can deliver to destination (Fig 2.a).

b. During Attack: Malicious node send signals that they know the address of the destination end. After that all the malicious nodes create a loop (Fig. 2.b).

c. After Enhanced CBDS Application: Applying Enhanced CBDS technique it will send alarm packets to all the nodes about the malicious node. Nodes will not send any packet to the malicious nodes – Red color (Fig. 2.c).

Results in Byzantine attack:

i. Throughput and Malicious node ratio: This result shows the ratio of PDR and Malicious node ratio. PDR is packet delivery ratio. PDR means ratio of the number of packets received at the destination and the number of packets sent by the source (Fig. 3.a).

ii. End to end delay and malicious node ratio: This result shows the ratio between End to end delay and malicious node ratio. End to end ratio means average time taken for a packet to be transmitted from the source to the destination (Fig 3.b).

iii. Throughput and Malicious node ratio: Throughput means average time taken for a packet to be transmitted from the source to the destination. Below figure shows the graph between throughput and malicious node ratio (Fig 3.c).

Fig. 3.a PDR and Malicious node ratio

Fig. 3.b End to end delay and malicious node ratio

Fig. 3.c Throughput and malicious node ratio

B. Resource Consumption Attack:

Resource consumption attack can be detected by adding new security checks to the algorithms. If the battery and bandwidth usage of any node are not going as per optimized usage thresholds set.

Fig. 4.a Ideal Case

Fig. 4.b During Attack

Fig. 4.c After Enhanced CBDS

i. Ideal Case: Green is the source node and blue is the destination node. Source sends the signals to the destination node after some interval of time (Fig. 4.a).

ii. During Attack: During attack malicious node connects to the source node and it takes all the bandwidth during that time. Red node is malicious node (Fig. 4.b).

iii. After Enhanced CBDS Application: Here we are applying Enhanced CBDS application technique to detect the malicious node, so that no packet will send to the malicious node (Fig. 4.c).

Results in Resource Consumption Attack:

Fig. 5.a PDR and Malicious node ratio

Fig. 5.b End to end delay and Malicious node ratio

Fig. 5.c Throughput and Malicious node ratio

i. PDR and Malicious node ratio: Fig. 5.a shows the ratio of PDR and Malicious node ratio. PDR is packet delivery ratio. PDR means ratio of the number of packets received at the destination and the number of packets sent by the source.

End to End delay and Malicious node ratio: Fig. 5.b shows the ratio between End to end delay and malicious node ratio. End to end ratio means average time taken for a packet to be transmitted from the source to the destination.

Throughput and Malicious node ratio: Fig.5.c shows the graph between throughput and malicious node ratio, where Throughput increases.

VI. Conclusion

Through proactive detection and reactive response at subsequent steps to minimize resource wastage, the Cooperative Bait Detection Scheme provides the hybrid approach. The implementation of Enhanced CBDS technique, it involved sending bait RREQ packets which contains the address of the adjacent one-hop neighbor node as destination address, we were successfully able to trace malicious nodes (nodes other than one-hop neighbor that sent RREP packets). Our results show that through the application of CBDS approach end to end delay value gets reduced & at par with values for "Before Attack Case". On the same lines throughput and PDR were also resumed at par with the "Before Attack Case"

References

- [1] Jian-Ming Chang, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao, and Chin-Feng Lai, Member, IEEE. "Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach." Published in Systems Journal, IEEE, 09 January 2014, pp. 1-11.
- [2] Yanwei Wang, F. Richard Yu, Senior Member, IEEE, Helen Tang, Senior Member, IEEE, and Minyi Huang, Member, IEEE. "A Mean Field Game Theoretic Approach for Security Enhancements in Mobile Ad hoc Networks." Wireless Communications, IEEE Transactions on (Volume:13, Issue: 3), March, 2014, pp. 1616-1627.

- [3] Seyed Mohammad Asghari Pari, Mohammad Noormohammadpour, Mohammad Javad Salehi, Babak Hossein Khalaj, Hamidreza Bagheri, Marcos Katz. "A Self-Organizing Approach to Malicious Detection in Leader-Based Mobile Ad-hoc Networks." Wireless Days (WD), 2013 IFIP, Valencia, 13-15 Nov. 2013, pp. 1-3.
- [4] Rashid Sheikh, Durgesh Kumar Mishra, Mahakal Singh Chandel, "Security Issues in MANET: A Review." in Wireless And Optical Communications Networks (WOCN), 2010 Seventh International Conference, Colombo, 6-8 Sept. 2010, pp. 1 - 4.
- [5] Wenjing Lou, Wei Liu Yuguang Fang "SPREAD: Enhancing Data Confidentiality in Mobile Ad Hoc Networks." Published in INFOCOM 2004. Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies (Volume:4), 7-11 March 2004, pp. 2404 - 2413 vol.4
- [6] P.-C. Tsou, J.-M. Chang, H.-C. Chao, and J.-L. Chen, "CBDS: A cooperative bait detection scheme to prevent malicious node for MANET based on hybrid defense architecture," in Proc. 2nd Intl. Conf. Wireless Commun., VITAE, Chennai, India, Feb. 28–Mar., 03, 2011, pp. 1–5.

Author Profile

Muskan Sharma received the B.Tech. degree in Computer Science & Engineering from Indo Global College of Engineering in 2011 and pursuing M.Tech (2014) from Swami Devi Dyal Institute of Engineering & Technology. Now she is working on her Master's Thesis on MANET. She is exploring Enhanced CBDS technique to detect the attacks like Resource consumption & Byzantine attacks.

Chander Prabha received the B.Tech. Degree in Computer Engineering from MMEC, Mullana in 2002 and M.E. from Punjab Engineering College (PU, Chd). Now she is working as an Assistant Professor (CSE) & Head of IT Department in SDDIET, Barwala, Panchkula. Her field of interest in the area of Wireless Networks, Multi Hop Networks Collaborative and Distributive Computing and Network Security.