International Journal of Grid and Distributed Computing
Vol. 13, No. 2, (2020), pp. 546 – 557

Evaluating Packet Detetction Attack for Improving the Delivery Ratio Using Cyclic Frame Redundancy Bit Analysis in Manet

1Raja Krishnamoorthi,

Professor, Department of ECE, CMR Engineering College, kandlakoyaVillaga, Hyderabad, Telangana-501401, India, krajameae@gmail.com.

2Dr.G.Suresh,

Professor, Sri Indu College of Engineering and Technology, Hyderabad.

geosuresh@gmail.com.

3Dr.P.Epsiba,

Associate Professor, Pallavi Engineering College, Hyderabad.

epsipaul.pallavi@gmail.com

4Dr.N.C.Sendhilkumar,

Professor, Sri Indu College of Engineering and Technology, Hyderabad.

sendhilkumarnc@gmail.com

Abstract

Packet drop attack MANETS are more familiar with security risks. This attack is important and inevitable because it is the practice of knowing any path to activate the loophole which brings with it the characteristics of envy. However, some of these networks lack of centralized management, the impact of security attacks. The specific attack is a black hole attack, in which the compromised reference packet is malicious. Rejection malicious packet attacks have become more common. Malicious nodes can be partially minimized or completely eliminated to disrupt communication on the network. Cyclic Frame Redundancy Bit Analysis Method (CFRBA) has been worked out. In this system, data from each node in the network is transported to a central location. The collected data from different nodes can be analyzed separately to detect the PDA (Packet Detection Attack). The CFRBA detection method is initiated for each change to the network topology of additional advantage in the case of a highly variable network of tracks. A new framework for predicting packet loss and congestion, based on end-end delay variance and trend measurement, helps avoid active error recovery and congestion. Based on the cooperation participation in the communication node, and the node's performance in the detection method, the trust value of the node is dynamically updated.

Keywords: *Mobile ad hoc network, Cyclic Frame Redundancy Bit Analysis Method, predict packet loss, packet detection attack.*

1. Introduction

It is used to detect sync phasor data packets that drop attacks on the Internet. The underlying challenge (which is caused by the crisis) is to distinguish those droplets that occur naturally in the network. The proposed mechanism is used to detect the purpose of synchronous phasor data packages experiences one-way delays in extracting the packet drop attack. A large number of imitations confirmed the efficiency of

ISSN: 2005-4262 IJGDC

the proposed detection mechanism. The rogue node drops data packets, which deliberately degrades network performance.

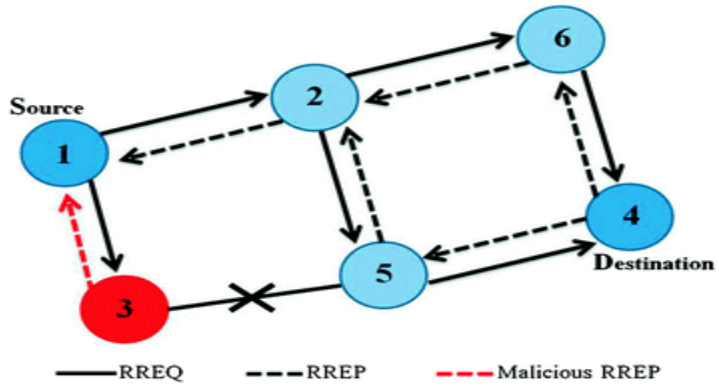


Figure 1 Packet Dropping Attack [22]

A wireless ad hoc network is a different attack, which is a general attack access to each layer of the routing mechanism acting as a network or topology on it. The attack has two purposes: it avoids changing the number of factors such as serial number, or it can not send packages. Hitting the node will stop the black hole. In this case, the node will continue to establish the path from the target source so that it acts as one of the intermediate nodes. For example, figure 1 shows the source node 1 sending an RREQ message, wait until it responds from any other node and then from other neighboring nodes, it will get a malicious RREP packet from the source which will upgrade its higher serial number and will know the new path to the source node that the target is established. In this case, the opponent can be retained in the system as long as the source is derived from the RREP source. Therefore, the key packet is lured to the node in such a way that it does not reach the target node, losing the packet.

Anomalous nodes also discard messages to save energy. A malicious node discards a data packet that requires forwarding to its neighbor. An attack is suspected when a neighbor drops a packet on a certain amount. Packet loss is considered RREQ, RREP packets, and data packets. Through the data transfer process, it is transferred to the target by establishing the data packet path. In the presence of malicious node functionality, the routing and data transfer routing protocol function is compromised. In a trusted environment, it operates using routing protocols and is expected to fully guide the packets.

Selective packet drop-off attacks are a type of service attack denial. The bandage loss attack is initiated during the advance phase. So this is very complicated and difficult to separate. This attack is easy to carry out, but difficult to detect. Selfish nodes also drop packets differently. They dropped their packets and saved their resources without harming the only other node. Selective transfer attacks can damage some tasks in application. In these types of attacks, malicious nodes operate as normal nodes each time, but selecting and releasing data packets involves different force movements that come with the main data packets. This fall is hard to detect. Countermeasures selective transfer attacks do not require malicious node identification or pattern synchronization.

Much work has been done to estimate the MANET later this year, especially when the delay performance parameters are complete. Basically, three methods have been proposed to estimate performance parameters: measurement, simulation, and analysis model; each of them has its advantages and disadvantages. The measurement method is to establish an actual MANET visual test site from the front of the given node (source) and measure the final to final delay. In sync with the best time component (high accuracy with negligible overhead), final to final delay measurement can be easily achieved by using two time seals at the source and target nodes. However, in large networks, global time synchronization is very expensive in terms of bandwidth and program memory consumption. Delay estimation is, therefore,

ISSN: 2005-4262 IJGDC

impossible to estimate end-to-end delay in single-hop mode and its extensions in multi-hop situations. It is not possible to characterize the input to intermediate nodes.

Given the routing information, it can also integrate link planning delays and reduce end-to-end delays. Depending on this planning strategy for relay node data packet exchange, there is a required storage transfer delay and connection planning delay. When the timeslot used by the output link has elapsed, the link scheduling delay is introduced immediately after passing through the timeslot used by the input link.

2. Related Work

The mobile ad hoc network is completely free of recognition of existing infrastructures or new companies, so these mobile nodes are defined on the ground, so they need to communicate with each other and start sending or receiving data packets as soon as possible. From a security standpoint, the mobile node connection through the wireless connection is protected against internal or external attacks, as the network can move at any time [1].

Transfer details from a source to target packets or in the form of data packets or control packets. This is a set of moves on other mobile devices from one direction that is not statically stable, and that MANET [2] does not require infrastructure to set any prefixes. Therefore, MANET requires specific security with different methods to detect duplicate inputs of terminals that are not working properly. Suppose the nodes work together reliably and correctly as the network works. To identify and detect packets that drop nodes using Support Vector Machines (SVMs) [3].

MANET is a wireless network application and does not require any self-installed infrastructure. If and then, all nodes within the same square metric change so that the MANET node communicates with all other nodes. Nodes this distribution can be MANET change attacks, packet drop attack or blackout attacks, and some potential attacks [4] which are at risk of recurrence.

Recently, many trusted routing algorithms have been introduced, but all have their limitations. Trust relationships are a menacing task for wireless ad hoc networks. In this network, preferably, Noord is a reliable way of collaborating at work. Based on the new secure trust routing scheme, it combines social and QoS trust [5]. A data packet that drops a node does not attract nodes adjacent to the dropped data packet in a black hole attack. It develops pre-possibilities with the help of the packet drop problem and the continuous Bayes theorem [6] during the MANET.

Ad-hoc networks allow nodes to connect dynamically and disappear from the network at some point. This standard feature of MANET has made it possible to attack vulnerable defenses. Spatial hypothetical connection attacks are a security risk. In this attack, a malicious node announced the shortest path with unreliable impacts [7] and target node interference communication. In a black hole attack, the packet drops so that the attacker instead sends it to its final target. It [8] is improving data transfer between mobile nodes to detect and prevent unexpected attacks.

DoS attack is a type of jellyfish attack because its prey-seeking behavior is very difficult. Jellyfish attacks are considered to be more difficult to detect as overall network performance decreases [9]. The fixed-point (mixed party) theory, semi-born-dead processes, and relay buffer are used as the controlled distribution model of the embedded Markov chains, followed by the Markov chain theory characteristic packet transmission processing. E2E developed a complete theoretical framework for late analysis [10].

The issue of optimal capacity (optimal capacity delay trade-off) remains open with various delay constraints. [11] To this end, graph characteristics from the fundamental relationships between relevant mobility drill-downs, network performance, and scheduling parameters. Knowledge delay for hop-to-packet can significantly improve network visibility and facilitate network scaling and management [12]. Tama Advanced Output Delay adds a small overhead to each path off the trade on the network side.

ISSN: 2005-4262 IJGDC

Networking speculations continue to propel nodes and base stations, at different speeds, at different densities, and faster / slower wireless vehicles with isolated/operating models of different assumptions [13].

The first application of the steering algorithm is to determine a single hop neighbor on the narrow path between the resource and the target. It then provides up-to-date routing information along the routing path [14] and performs periodic local flooding caused by the destination node. Trust-based Probabilistic Broadcasting (TPB) is particularly focused on reducing overhead by malicious nodes where rebroadcast possibilities are based on node reliability results. To achieve the terminal's confidence level, the lightweight trust management model is designed based on direct and recommended confidence sources [15].

The MAC (Media Access Control) protocols are installed, which help to approximate MAC alternate points and the analytical model of the closed format. Furthermore, the connection between mobile environments and disruptive networks presents [16] major challenges in the utilization of central network content. [17] This content considers the potential of using mobile users in improving distribution efficiency. Optimized overhead scheduling strategy for multitasking devices in ad-hoc is used for mobile edge computing systems. The planning strategy for this task takes the opportunity to reduce overhead on each mobile device [18] by taking into account consumption, delayed energy consumption, and cash outlay.

Data transmission without errors is an essential function in the MANET transmission. With the characteristics of energy spreadsheets and distributed architecture, multimedia routing at-the-hock networks will make great strides in wireless. Multiple navigation methods can be used to detect multiple data packets dropped by adjacent nodes in network traffic jams [19-20].

3. Implementation of Proposed Work

Communication between them, the most desirable characteristic of mobile ad hoc networks, is node collaboration. Non-cooperation nodes make an exception for the network. Therefore, restricting the collaboration of wireless ad hoc networks created by uncooperative malicious nodes improves network usability. Here, for the sake of simplicity, let's a group of malicious nodes in the network that tried to discard them; otherwise, it is possible that a forwarding packet to all destinations would disrupt network operation. To mitigate the unexpected behavior of this type of network, real nodes try to ally with them. The goal formed by the true node alliance is to detect malicious nodes that improve network utilities, so launch attacks reduce network utilities in terms of data rates.

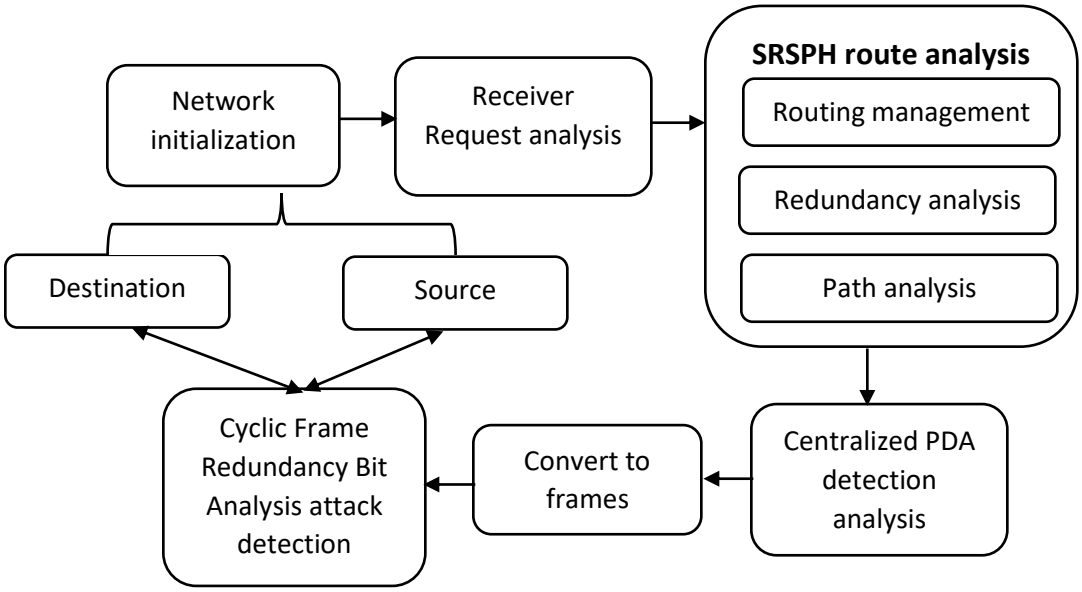


Figure 2 Implementation of the Proposed System Block Diagram

ISSN: 2005-4262 IJGDC

Figure 2 illustrates the reliable node-to-end communication overview of this CFRBA working contribution MANET data packets through several sections to functional groups. If the network utility turns out to be in the expected range, the suspicious node may or may not be malicious. At this point, the suspect node will stay in an alliance because node trust can happen because there is no network congestion, malicious packet loss is reduced, and trying to lose packets can occur.

3.1 Centralized PDA Detection

With the centralized PDA detection method, the nodes in the network use the information they collect to provide a central entity. The central entity parses the information received from a particular node at a particular node to detect the PDA on its own. Central location for ship data analysis. It implements a statistical detection method. The host computer will review this. The existing method is not scalable and thus suffers from the central analyzer's inefficient capacity under heavy network load. The centralized PDA detection method can detect malicious nodes from centralized data collection. It has a relatively small number of components that need to keep running. If packet loss exceeds the PDA threshold, packet loss is suspected. PDA is based on some network performance parameters at a particular node, such as packet transfer rate and network throughput. It assumes that the packet needs to be forwarded in a special way, hop-by-hop. The communication link is free of radio channel errors that are not assumed to be bidirectional.

Algorithm Steps:

Input: Details of Number of PacketsN_n, T_M is the minimum throughput and D_P drop of data packets.

Output: PDA detection in network communication between source and destination.

Identify the sending data packets details to count.

$$For\ all\ (i\ in\ N_n)\ do$$

Find T_t amount of packets send from the number of data packets received denoted as T_r, T_d dropping of the data packets.

End for

Compare the number of data packets sending and receiving between the neighbor nodes.

$$For\ all\ (i\ in\ N_n)$$

Recognition of PDA

$$for\ all\ (i\ in\ N_n)\ do$$

end for

T, is the Throughput and d is the numbers of packets delivered t within t times for a node i

$$T_t\ =\ \frac{d}{T}$$

end for

$$if\ ((PDRi\ >\ PDRth)\ AND\ (T,\ <\ Tth))\ then\ \{'"\ PDRth\ is\ the\ threshold\ packet\ drop\ ratio\ for\ a\ node\ i\ "'\}$$

End if

If the packet loss is higher than the threshold, the PDA is suspected of losing more packets. Probably, a PDA is based on different network performance parameters such as packet transfer rate and

ISSN: 2005-4262 IJGDC

network performance specific nodes. It assumes that the packet must be sent specially by hop-by-hop. The communication channel is free of radio channel errors that are not considered two-sided. All terminals use one-way antennas for two-sided communication. Neighbor Discovery protocols operate in such a way that each node learns about the neighbor associated with it.

3.2 Secure Reactive Shortest Path Routing (SRSPH) route analysis

Deviating from this target data packet source is also a safe reaction shortcut to diversion to study time differences. This includes all types of intermediate hop delays that come for any reason of the packet. This is usually from the source due to intermediate hops, route detection delay effects, port queues, retransmission delays, and other systems proposed to get end-to-end delay queuing to achieve a node. Consists of different types of destination calculations or security measures. RREQ A small delay to and from the flooding phase. When the RREQ packet reaches the target node towards its first target, it calculates the overall wiring delay. The destination node sends an RREP message late. On the lower edge of the dead from the source node to choose the environment chooses them.

Step1: If (node = =source)

Then sort (routes) using minimum (the delay)

Else rebroadcast (RREP)

End if

To minimize minimum delay: Minimize max

$$delay = a_0 + \sum_{n=REQ}^{\infty} (d_i)$$

Step2: REQ is the REQ packet sent to all neighbors of the node that suspects End to end.

if (node> p_i) AND (n_i) then

Neighbor checks it's for shortest path

Forward RESP to the original sender

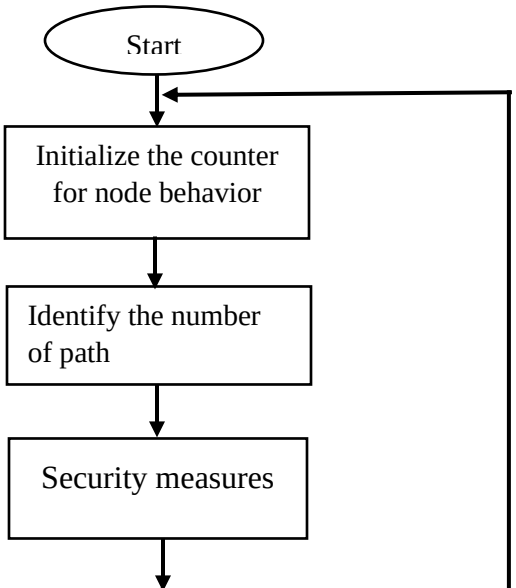
Until the communication belongs to one source can be connected to become a complete data flow.

Where,

p_i - denotes the path

REQ- Requests

RESP- Response



ISSN: 2005-4262 IJGDC

Figure 3 SRSPH route analysis

The source node floods the routing request to the destination node route analysis flow is shown in figure 3. If a node is reached by a neighbor or a node depends on a request message, the node route notifications should find the route request delay. The target node finds the total delay, updated with the response message. When the source node receives a response, low delay, and chooses the best path. The packets were exported proportionately because these CFRBA got the best results.

3.3 Cyclic Frame Redundancy Bit Analysis (CFRBA)

The Cyclic Frame Redundancy Bit Analysis to identify the node attack in WSN network the proposed prevention protocol. If any node receives a link request which initially searches its data frame for information about requesting node whether there is trace as local data or global data. Local data is a one hop neighbor transaction information and global data is multichip remote node transaction information. The details of the structure are used to control whether the requesting node is an attack or not. If the requested node is attacked, the detailed data frame conflicts, not due to global data with the requested location. Also the activeness of the multi-hop remote node is ensured and to confirm the requesting node is attacked. In the case of data frame miss, the random w witnesses are chosen which initiates a bit wise analysis. The frames will redirect requests if there is no required information is present in global data. Again the next set of random g witnesses is chosen to initiate the next bit analysis.

Algorithm steps:

Input: request Hello Message (Msg), Packet size (Ps), frame count (Fc).

Output: data transmission permission and attack detection

For i=0 to each node (n)

If request n (i) then scan Msg (n_i) < th value // th is threshold value

Cover to bit (Msg)

Fc=$\sum_{msg}^{n}$ $bit++$;

Get link between n_i and n_{i+1}

ISSN: 2005-4262 IJGDC

End

If Msg (n_i) then $Nei_b(n_i)$ // to compare to neighbor node (Nei_b) message

its $Nei_b(n_i)$ match then its trusted node

Else

Choose the another cycle;

End for

The frame replacement policy is initiated when the bit is filled. The status of the requesting node such as attacked or benign and its activeness, witness's activeness are updated in each frame as when the state changes occurred.

4. Result and discussion

A Network Simulator (NS2) is used to simulate all types of networks. It is a unique event-driven simulator that starts sending packets at a specific time. The results are generated in a graphical form. Performance measurements are evaluated to verify the proposed system.

Table 1 Simulation Parameters

Parameters	Value
Data rate	2 Mbps
Application Type	Constant bit rate (CBR
CBR interval	1.0 (second)
Simulation Time	350 s
Simulator	NS-2
Node Speed	20 m/s

Table 1 shows with the resources required in the proposed system. The result and discussion describes the comparison of existing TPB (Trust-based Probabilistic Broadcast scheme), APD-JFAD (Accurate Prevention and Detection of Jelly Fish Attack Detection), FHSS (Frequency Hopping Spread Spectrum) and CFRBA method.

The comparison parameters are given below:

Package Delivery Ratio - ratio between the clients of the packet is the number of packets first received by the CBR source of the application layer and the final target via the CBR sink.

ISSN: 2005-4262 IJGDC

End to End Delay- This is the general expectation between the information provided by the CBR resources and the associated CBR recipient invoice.

Packet Drop Analysis: If the Packet Drop Ratio (PDR) for a particular node is too high, and the performance is too low, it is suspected to be malicious. It is assumed that the nodes in the wireless channel communicate with each other and that there is a partial packet drop due to congestion, excessive load, or media interference. The flow of traffic will be monitored by each node participating in the communications. Agents will perform a local analysis of the packet fall at each end.

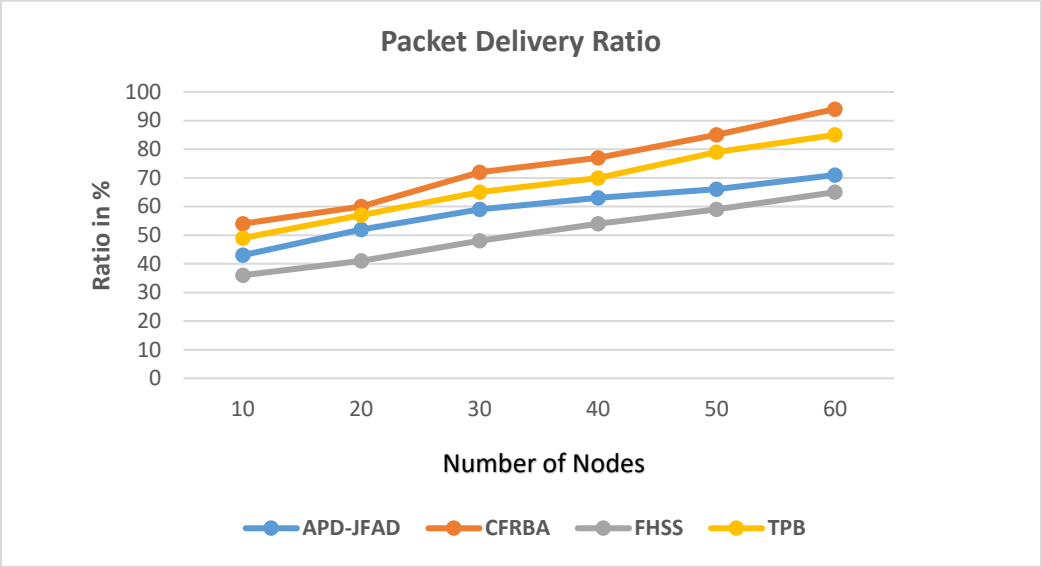


Figure 4 Packet Delivery Ratio

Figure 4 shows a comparison of the Packet Delivery Ratio (PDR). As a model number of data packets of the receiving node is sent to the receiving node.

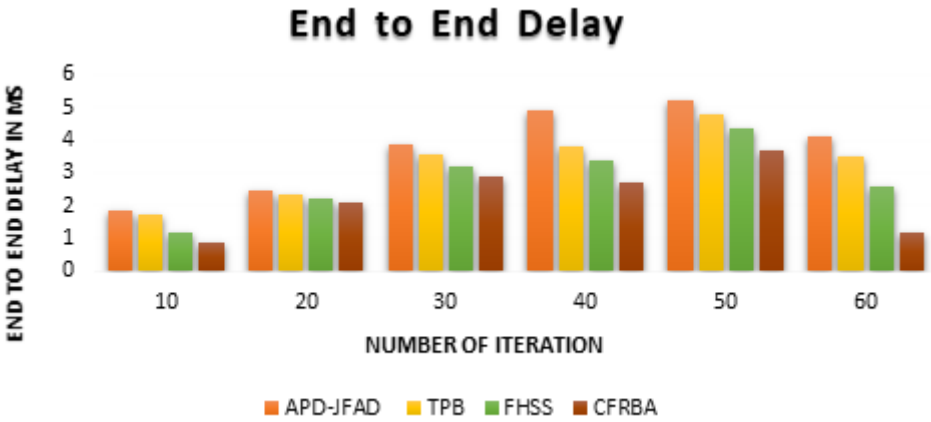


Figure 5 End to End Delay Analysis

Figure 5 shows the node End-to-End Delay .The first node is a typical delay, the stabilization node message which turns out to start in a few minutes, waiting in the product packet. End to End delay of the CFRBA 1.2 in ms, compared to the existing APD-JFAD 4.1 in ms, TPB 3.5 in ms, FHSS 2.6 in ms methods.

ISSN: 2005-4262 IJGDC

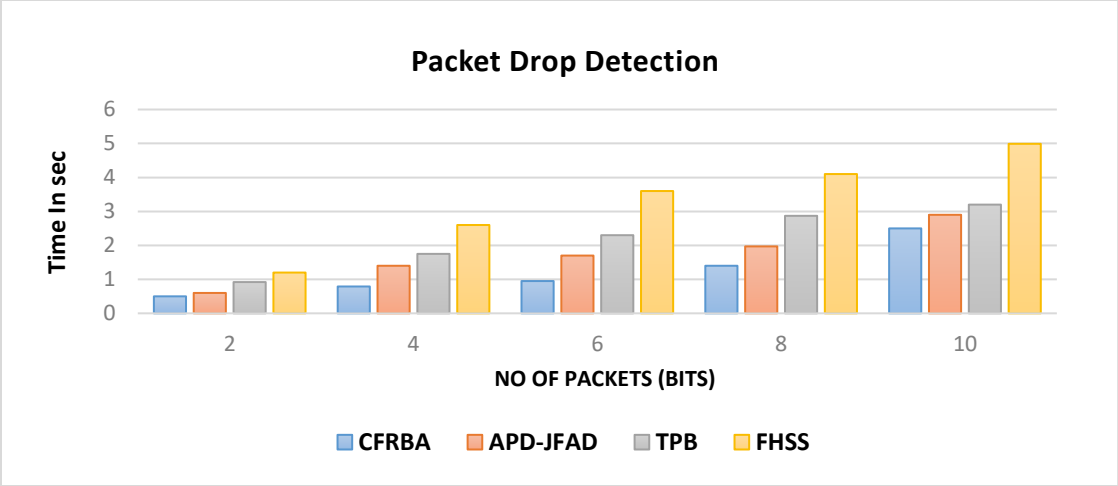


Figure 6 Packet Drop Detection

Figure 6 shows that the evaluation of packet drop detection analysis in the proposed CFRBA 2.5 with sec and then the existing methods APD-JFAD 2.9 with sec, TPB 3.2 with sec, FHSS with 4.99 sec.

Table 2 Throughput Performance

Simulation Time in s	FHSS in bps	APD-JFAS in bps	TPB in bps	CFRBA in bps
0	0	0	0	0
10	174	192	210	234
20	246	264	288	306
30	312	348	384	396
40	504	516	522	528
50	546	558	576	588

Table 2 indicates the throughput values received throughout simulation analysis for APD-JFAD, TPB, FHSS and CFRBA.

Successfully spreading the process, and sending data packets of as many as 200 data packets to the Internet. Throughput is obtained using equation 3.3.

$$Throughput = \frac{Packets\ Received\ (n) * Packet\ size}{200} \quad \text{---} \quad (2)$$

Where
n = number of nodes

ISSN: 2005-4262 IJGDC

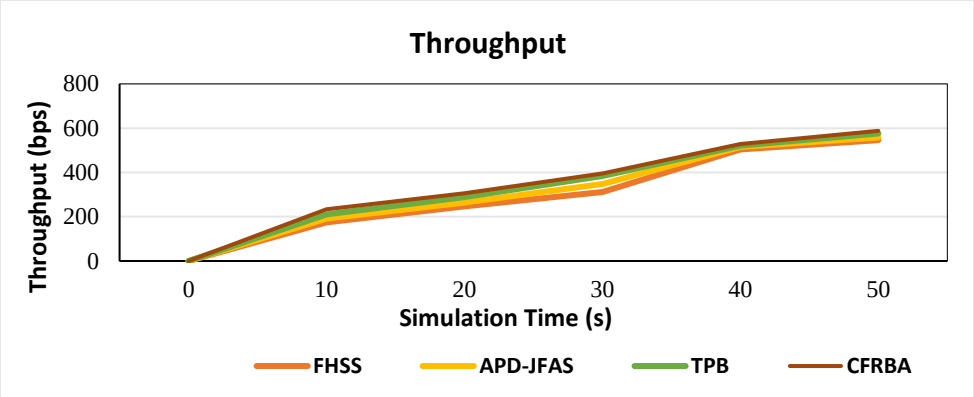


Figure 7 Analysis of throughput performance

Action message refers to the amount of information that is effectively transmitted between the source node and the target node. It can be successfully received from the number of data packets in figure 7, every 200 data packets are observed for CFRBA is higher than compared 588 in bps to that of the existing algorithms FHSS 546 in bps, APD-JFAS 558 in bps, TPB 576 in bps.

5. Conclusion

In ad hoc networks, node cooperation is the most desirable feature of communication between them. The CFRBA system is a malicious data packet where the packet loss rate is low, or that other packets are the other hypothesis is the threshold packet loss. Analyze if it exceeds. If packet loss exceeds the PDA threshold, packet loss is suspected. A PDA is suspected to be a particular node based on different network performance parameters like packet transfer rate and network throughput. It assumes that the packet needs to be forwarded specially, hop-by-hop. Interleaving is a useful technique to reduce the effects of loss when the cell size is smaller than the packet size, and end-to-end delay is not important. MANET is the desired destination for node-to-node delay data packets from the last stage. Based on the proposed delay, it is the current method of comparing edges from scars that end the proposed delay. CFRBA to given the performance of packet delivery ratio value is 85%, end to end delay analysis 1.2 sec, packet drop detection in 2.5 sec and the and throughput level is 588 bps.

References

1. Chaudhary, A., Kumar, A., & Tiwari, V. N. (2014). A reliable solution against Packet dropping attack due to malicious nodes using fuzzy Logic in MANETs. 2014 International Conference on Reliability Optimization and Information Technology (ICROIT). doi:10.1109/icroit.2014.6798326.
2. Soliyal, N., & Bhadauria, H. S. (2016). Preventing packet dropping attack on AODV based routing in mobile ad-hoc MANET. 2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI). doi:10.1109/icacci.2016.7732239.
3. Parihar, R., Jain, A., & Singh, U. (2017). Support vector machine through detecting packet dropping misbehaving nodes in MANET. 2017 International Conference of Electronics, Communication and Aerospace Technology (ICECA). doi:10.1109/iceca.2017.8212711.
4. Nagendranath, M. V. S. S., Ramesh, B. ., & Aneesha., V. (2017). Detection of Packet Dropping and Replay Attacks in MANET. 2017 International Conference on Current Trends in Computer, Electrical, Electronics and Communication (CTCEEC). doi:10.1109/ctceec.2017.8454918.
5. Shah, S. N., & Jhaveri, R. H. (2016). A trust-based scheme against Packet dropping attacks in MANETs. 2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT). doi:10.1109/icatcct.2016.7911967.

ISSN: 2005-4262 IJGDC

6. Kshirsagar, V., Kanthe, A. M., & Simunic, D. (2014). Analytical approach towards packet drop attacks in mobile ad-hoc networks. 2014 IEEE International Conference on Computational Intelligence and Computing Research. doi:10.1109/iccic.2014.7238292.
7. Jain, A. K., & Patidar, J. (2018). Detecting Packet Dropping Misbehaving Nodes in MANET Using RTT. 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI). doi:10.1109/icoei.2018.8553845.
8. Vhora, S., Patel, R., & Patel, N. (2015). Rank Base Data Routing (RBDR) scheme using AOMDV: A proposed scheme for packet drop attack detection and prevention in MANET. 2015 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT). doi:10.1109/icecct.2015.7226060.
9. Doss, S., Nayyar, A., Suseendran, G., Tanwar, S., Khanna, A., Son, L. H., & Thong, P. H. (2018). APD-JFAD: Accurate Prevention and Detection of Jelly Fish Attack in MANET. IEEE Access, 1–1. doi:10.1109/access.2018.2868544.
10. Liu, J., Sheng, M., Xu, Y., Li, J., & Jiang, X. (2016). End-to-End Delay Modeling in Buffer-Limited MANETs: A General Theoretical Framework. IEEE Transactions on Wireless Communications, 15(1), 498–511. doi:10.1109/twc.2015.2475258.
11. Jia, R., Yang, F., Yao, S., Tian, X., Wang, X., Zhang, W., & Xu, J. (2017). Optimal Capacity–Delay Tradeoff in MANETs With Correlation of Node Mobility. IEEE Transactions on Vehicular Technology, 66(2), 1772–1785. doi:10.1109/tvt.2016.2564423.
12. Gao, Y., Dong, W., Chen, C., Zhang, X., Bu, J., & Liu, X. (2017). Accurate Per-Packet Delay Tomography in Wireless Ad Hoc Networks. IEEE/ACM Transactions on Networking, 25(1), 480–491. doi:10.1109/tnet.2016.2594188.
13. Luo, Z., Gan, X., Wang, X., & Luo, H. (2016). Optimal Throughput–Delay Tradeoff in MANETs With Supportive Infrastructure Using Random Linear Coding. IEEE Transactions on Vehicular Technology, 65(9), 7543–7558. doi:10.1109/tvt.2015.2481427.
14. Choi, H.-H., & Lee, J.-R. (2019). Local Flooding-Based on-Demand Routing Protocol for Mobile Ad Hoc Networks. IEEE Access, 7, 85937–85948. doi:10.1109/access.2019.2923837.
15. Xu, H., Si, H., Zhang, H., Zhang, L., Leng, Y., Wang, J., & Li, D. (2020). Trust-Based Probabilistic Broadcast Scheme for Mobile Ad Hoc Networks. IEEE Access, 8, 21380–21392. doi:10.1109/access.2020.296944.
16. Ye, Q., Zhuang, W., Li, L., & Vigneron, P. (2016). Traffic-Load-Adaptive Medium Access Control for Fully Connected Mobile Ad Hoc Networks. IEEE Transactions on Vehicular Technology, 65(11), 9358–9371. doi:10.1109/tvt.2016.2516910.
17. Tianze, L., Muqing, W., Min, Z., & Wenxing, L. (2017). An Overhead-Optimizing Task Scheduling Strategy for Ad-hoc Based Mobile Edge Computing. IEEE Access, 5, 5609–5622. doi:10.1109/access.2017.2678102.
18. Islam, H. M. A., Chatzopoulos, D., Lagutin, D., Hui, P., & Yla-Jaaski, A. (2017). Boosting the Performance of Content Centric Networking Using Delay Tolerant Networking Mechanisms. IEEE Access, 5, 23858–23870. doi:10.1109/access.2017.2765379.
19. Robinson, Y. H., Julie, E. G., Saravanan, K., Son, L. H., Kumar, R., Abdel-Basset, M., & Thong, P. H. (2019). Link-Disjoint Multipath Routing for Network Traffic Overload Handling in Mobile Ad-hoc Networks. IEEE Access, 1–1. doi:10.1109/access.2019.2943145.
20. Jeong, C., & Shin, W.-Y. (2018). Network-Decomposed Hierarchical Cooperation in Ad Hoc Networks With Social Relationships. IEEE Transactions on Wireless Communications, 1–1. doi:10.1109/twc.2018.2868767.
21. Qin, J., Li, M., Shi, L., & Yu, X. (2018). Optimal Denial-of-Service Attack Scheduling With Energy Constraint Over Packet-Dropping Networks. IEEE Transactions on Automatic Control, 63(6), 1648–1663. doi:10.1109/tac.2017.2756259.
22. https://link.springer.com/chapter/10.1007/978-81-322-2728-1_33#:~:text=Fig.%202

ISSN: 2005-4262 IJGDC