International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

Detecting and Eliminating Blackhole Attacks for Improving the Quality of Service of Mobile Ad-Hoc Networks Using RTS-CTS Mechanism

Ganesh Dhondu Dangat *[1], Dr.S .Murugan [2]

Submitted: 07/02/2024 **Revised**: 15/03/2024 **Accepted**: 21/03/2024

Abstract: Mobile Adhoc Network is one of the infrastructures-less, decentralized wireless networks that can reconfigure by itself. MANET does not depend on the access points in the network, where it can accommodate any existing infrastructure. Since it is an ad-hoc network, all the nodes in the MANET are mobile nodes connected wirelessly. Depending on the routing protocols, single-hop, two-hop, and multi-hop-based data transmission is followed in the MANET. These models provide more opportunities for malicious activity creation in the network, where it destroys data transmission and loss. Several earlier research works have focused on detecting and eliminating malicious activities. One of the dangerous attacks that defy detection of the physical properties is the Blockhole attack, and they don't respond to its sender and receiver nodes. Compared to other malicious attacks, blackhole attacks result in a small amount of data loss in the network, and they are considered a major research problem in MANET. This paper has aimed to provide a better solution using the RTS-CTS mechanism and initialize the data transmission with dummy data to detect the black hole nodes. Once the black nodes are identified in the network, they are eliminated immediately, and their functionalities are with the neighbor nodes. The simulation results obtained from NS2 show that the proposed RTS-CTS mechanism outperforms and provides better QoS.

Keywords: *MANET, Blackhole Attack, RTS-CTS Mechanism, Detecting Malicious Activities, Preventing Network.*

1. Introduction

MANET is a wireless network of mobile networks that can communicate without fixed access points. It exploits the MANET nodes, which rely upon routing protocols to discover and maintain routes to other nodes, which becomes the default next hop for other nodes of the targeted network. The malicious node creates a false indication terming it as the shortest path to the destined node. It is known as a route poisoning attack. The attacker can use this technique to launch a DoS attack for malicious activities, gathering sensitive data, or malware distribution. Research literature has proposed several methods to detect and alleviate the impacts of blackhole attacks, which are given in Table 1.

A black attack is a cyber-attack that targets a specific network and consumes all of its available bandwidth. Networks with limited bandwidth have a high chance of being attacked. This is a severe threat as it completely shuts down the Internet available for all users of the targeted network. It brings enormous losses for businesses relying on the Internet. It is a type of denial of service (DoS) where the attacker propagates a false routing table to other routers on the Internet. It sends the traffic intended for the targeted network to the attacker's machine instead of the original destination. As the traffic reaches the attacker's machine, they discard the data. This activity results in the unavailability of the network to legitimate users and causes a black hole, where data sent to the destination is lost. Various Scenarios of blackhole attack creation in MANET are illustrated in Figure 1. These scenarios say that the black node may be one of the intermediate, center, or corner nodes in a route.

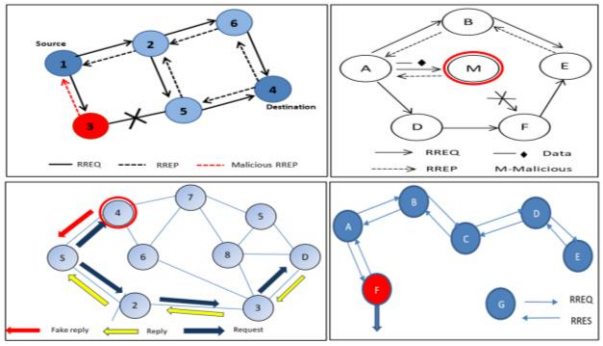

Figure-1. Various Scenarios of Blackhole Attack

Various security protocols are proposed to address the black hole attacks in the MANET network. These protocols have used the RTS and CTS mechanisms to transmit the data packets through the network efficiently. However, these protocols do not consider the nodes' performance through which the network's overall efficiency can be evaluated. The performance of each node counts in a system, and a protocol can be designed to analyze the performance of the individual nodes by utilizing the RTS-CTS mechanisms.

[1]*Research Scholar, Department of Computer Science, SIT Chennai.*
[1]*Assistant Professor, Karmaveer Bhaurao Patil College of Engg,.*
ORCID ID : 0000-0003-1340-1295
[2]*Professor, Department of Computer Science, SIT, Chennai.*
ORCID ID : 0000-0001-5503-8960
** Corresponding Author Email: ganesh.dangat@kbpcoes.edu.in*

Table-1. Traditional Methods for Blackhole Attack Detection

Methods	Description
Route discovery time	This method measures the route discovery time to the packet reaching the target node. If the time exceeds the expected time, a blackhole attack is possible.
Link quality	The quality of links between nodes is monitored to detect blackhole attacks, as a poor-quality link to the malicious node could detect possibilities of attack.
Path validation	This method sends a validation packet to the next hop, and the packet path is validated. Receiving the acknowledgment indicates the absence of a blackhole attack and vice-versa.
Collaborative detection	Information between nodes is shared so that if any node can't reach a particular destination, there can be possibilities of blackhole attacks.
Anomaly detection	This detection method monitors network traffic; if a particular node receives more packets, a blackhole attack could occur.
Using IDS or IPS	The blackhole attacks can be detected and prevented by using IDS or IPS.
Using honeypots	This is used to track attackers and trap them so that techniques used by attackers can be gathered.

ML and DL algorithms can now identify and eliminate the black nodes by blocking their' IP addresses. Combining these methods might help MANET to keep them away from blackhole attacks. An organization must update the network according to the latest security protocols and stay vigilant to protect the network. This paper contributes to,

- A scalable network is created in Network simulator -2 software and activates various conventional protocols, like AODV, MAODV, OLSR, etc., which are available.
- Implement the RTS-CTS mechanism with the scheduled data transmission process and deploy it in the simulation.
- Simulate Different scenarios to verify their performance and, finally, evaluate the performance at different scenarios.

Literature survey

This paper has focused on understanding the issues and challenges faced by the earlier methodologies. So, a detailed literature review is carried out and explained here. For example, Dhaka et al. (2015) presented a study to define various methods to handle the MANET's gray and black hole attack. Finding the malicious nodes in the MANET is one of the difficult tasks. Various literature reviews are discussed in this work to define the optimal solution. The malicious node in the MANET is identified based on the performance of the nodes.

One of the authors, Siddiqui et al. (2015), has introduced a secured Knowledge algorithm to prevent and detect black hole algorithms in MANET. The traditional AODV routing protocol is updated using the proposed algorithm to identify the malevolent nodes effectively. The experimental result of the proposed model indicates that the updated AODV protocol in the proposed secured knowledge algorithm more efficiently detects the black hole nodes in MANET than in the existing system. S. Naveena et al. (2020) suggested a trust-based routing algorithm to detect the blackhole attack in MANET. The proposed routing algorithm is classified into two stages to detect malicious nodes effectively. The two stages are data retrieval and route development, which are used to identify the malicious nodes securely. D.R. Choudhury et al. (2015) proposed a research work to improve the efficiency of the AODV routing protocol in the MANET system. The main focus of this research is to reduce the black attack in MANET with the help of the AODV routing protocol. The result of the research work emphasizes the proposed model performance better. S. Yadav et al. (2017) proposed a secured algorithm to safeguard the AODV routing protocol in MANET from black hole attacks. The simulation result observed from the simulator depicts that the proposed algorithm is more effective, simple, and robust in detecting the attacks than other methods. S.H. Mahin et al. (2019) proposed a DYMO routing protocol to detect the malicious attack in MANET. Based on the IDS, the black hole attack in MANET is identified by performing the proposed algorithm in MATLAB software. For this, KNN, SVM, DT, and neural network algorithms are evaluated, and the final result is calculated. The result indicates the proposed approach performs better.

P. Rani et al. (2020) discussed that MANET is a popular wireless technology that is more suitable for reducing complexity during communication. In MANET, various kinds of attacks are used, such as gray hole attack (GHA), sink hole attack (SHA), black hole attack (BHA), etc. Of these, BHA and GHA are discussed in this paper. The author proposed a swarm-based artificial bee colony optimization technique with an ANN algorithm to reduce the BHA and GHA. Using MATLAB software, the simulation result of the model is evaluated. The result shows that when compared with existing routing protocols, the proposed routing protocol performed better. H. Moudni et al. (2019) defined that though various detection techniques are used in wired and wireless MANET systems, the efficiency of those methods is satisfactory. So the author has proposed PSO and fuzzy-based system to detect the blackhole attack in the MANET. R. Thanuja and A. Umamakeswari et al. (2019) proposed the HPSO-GA technique to detect the attacks in MANET. The routing information is gathered using the data routing information node, and using the AODV routing protocol, the process is performed. The proposed HPSO-GA model effectively detects the blackhole attack in MANET. The efficiency of the model is analyzed based on the PDR, FPA, delay time, and throughput values. This proposed algorithm effectively reduces the delay time and routing overhead. S. Pandey and V. Singh (2020) suggested ANN and SVM methods to detect black hole attacks in MANET using the AODV routing protocol. The proposed model experiments with 100 nodes; the result of the experiment indicates that the proposed model improves the energy consumption, throughput, PDR, and delay with 54.72%, 88.68%, 92.91%, and 37.27ms, respectively.

The author G. Farahani (2021) has proposed that KNN and fuzzy inference algorithms have been used for clustering and cluster-head selection, respectively. The simulation result of the proposed model illustrated that the suggested model improves the overall performance of the blackhole detection techniques in the MANET. The packet loss rate, throughput, network delay, and PDR values are improved than the existing detection techniques. C. Joseph et al. (2015) presented the study to emphasize the performance of the MANET during the blackhole attack. Using the AODV routing protocol, the malicious nodes are detected and simulated with the NS2 simulator. The performance of the proposed model is evaluated by calculating and comparing some performance metrics. The model's simulation result shows that compared with other detection models, the proposed model effectively identified the black hole attack in MANET. V. Srinivasan (2021) introduced a new method: a honeypot agent-based detection scheme with long-term short-term memory (LSTM) to detect the malicious nodes in the network. The proposed HPAS-LSTM model effectively analyses the blackhole attack using the simulator NS2. The performance of the proposed model has proved to be better than the other existing models in terms of various performance metrics values such as TH, PDS, PLR, and TND.

From the above, it is noticed that recent literature has stated that AI methods provide better performance in network data analysis. Still, the data generation needs to be appropriate, and it should provide the node, data, and route behavior. It can be obtained only from the routing table based on the RTS-CTS mechanism. Hence, this paper has aimed to propose RTS-CTS mechanism-based routing in MANET.

Limitations and Motivation

The research on RTS and CTS mechanisms has proposed various optimization protocols that efficiently transmit packets through the network. However, the black hole attack discussed in the literature shows a decline in the performance of the nodes in the black hole region, leading to the corruption of the total network. To overcome such attacks, the protocols use the RTS-CTS frames between the source and destination to detect the abnormalities. However, the intermediate nodes in the network are important aspects for detecting the vulnerabilities. The data breaches in the middle nodes can surely affect the network and data packets. Most of the protocols proposed by the previous works have only considered the source and destination node and transmission parameters. They also failed to consider the performance of the individual nodes. Thus, there is a need for a protocol that can optimize the functioning of the intermediate nodes and also consider the performance parameters of the individual nodes to provide better protection from blackhole attacks in the network.

Proposed Architecture

This paper implements the RTS-CTS mechanism for identifying and eliminating the blackhole attack nodes in the network. The overall functionality of the proposed model is illustrated in Figure-2. It says that the protocol persists in the routing information in the routing table. From the routing table, all the information regarding the nodes acting as the intermediate nodes helps in processing the request, response, reply, message, data, acknowledgment, time of sending, time of receiving, etc. Based on the data from the routing table, verifying the node's activation and performance is easy. The node that does not have any data in the routing table is detected as a Blackhole attack in the network. The RTS-CTS mechanism generates all the information like Req, Res, and Reply used in this paper.

The proposed architecture consists of various nodes validated by the packet forwarding protocol that validates the usability of the node in the network. It can also be noted that, over each iteration, the sender and receiver are

selected, and the selected members are then sent to the protocol that validates the reliability of the nodes and sends the data to the protocol. It detects whether the node is affected by a black hole attack or not and passes them to compute the OOS factor. If the nodes are affected, they are eliminated and again diagnosed through the routing protocol. This cycle continues infinite times based on the requirements of the network.

Proposed protocol

The vehicular nodes are accurately positioned through the GPS, and it also periodically updates its position information. The topology of the road can be easily obtained from the available digital maps, and this information can be synced in real-time. However, during the simulation, the roads with dead ends are not considered. This paper proposes a packet forwarding protocol that forwards the data packets through various urban scenarios to detect network black hole attacks. In this protocol, the nodes are selected through the self-election process, which helps to overcome the RTS and CTS frames. As a MANET is a distributed dynamic network with different connection modules, the coordination of the nodes gets a hit due to the black hole attacks.

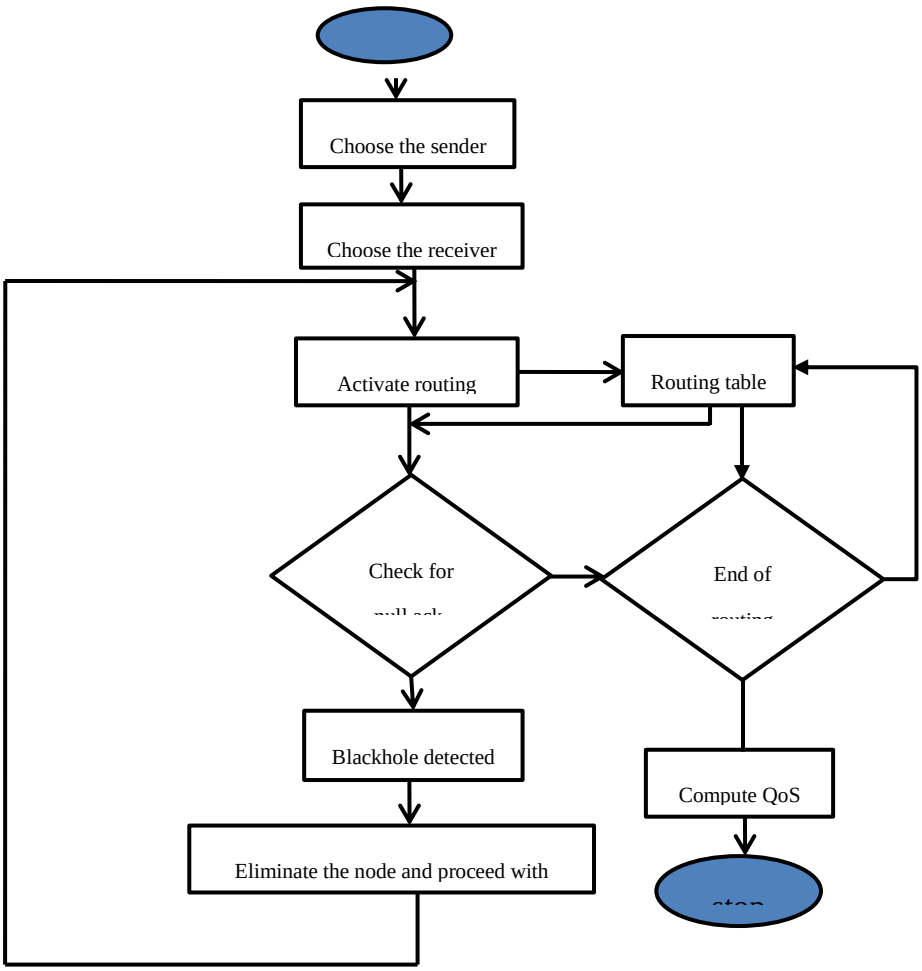

Fig-2. The proposed architecture of the protocol and functioning model

However, a distributed coordination function with various RTS and CTS sessions is proposed to improve the coordination between the nodes in a black hole region. A space timer is set to measure the time between the inter-frames while forwarding the data from the source to the destination nodes. It checks the state of the destination node before transmitting the data, and if the node is selected, the times are set to 0. However, when the time expires and if there is a failure in the transmission of the packets, the source node sends an RTS, and the destination node sends CTS to the router. When the time is set to 0, the data is automatically forwarded; however, if the time is greater than zero, the protocol searches for the ideal node. The proposed model adopts a distributed network with a multi-hop model. The data is transferred through various intermediate nodes, and the proposed model allocates the time required for transmitting the data between the nodes and the intervals between the neighbors during the transmission.

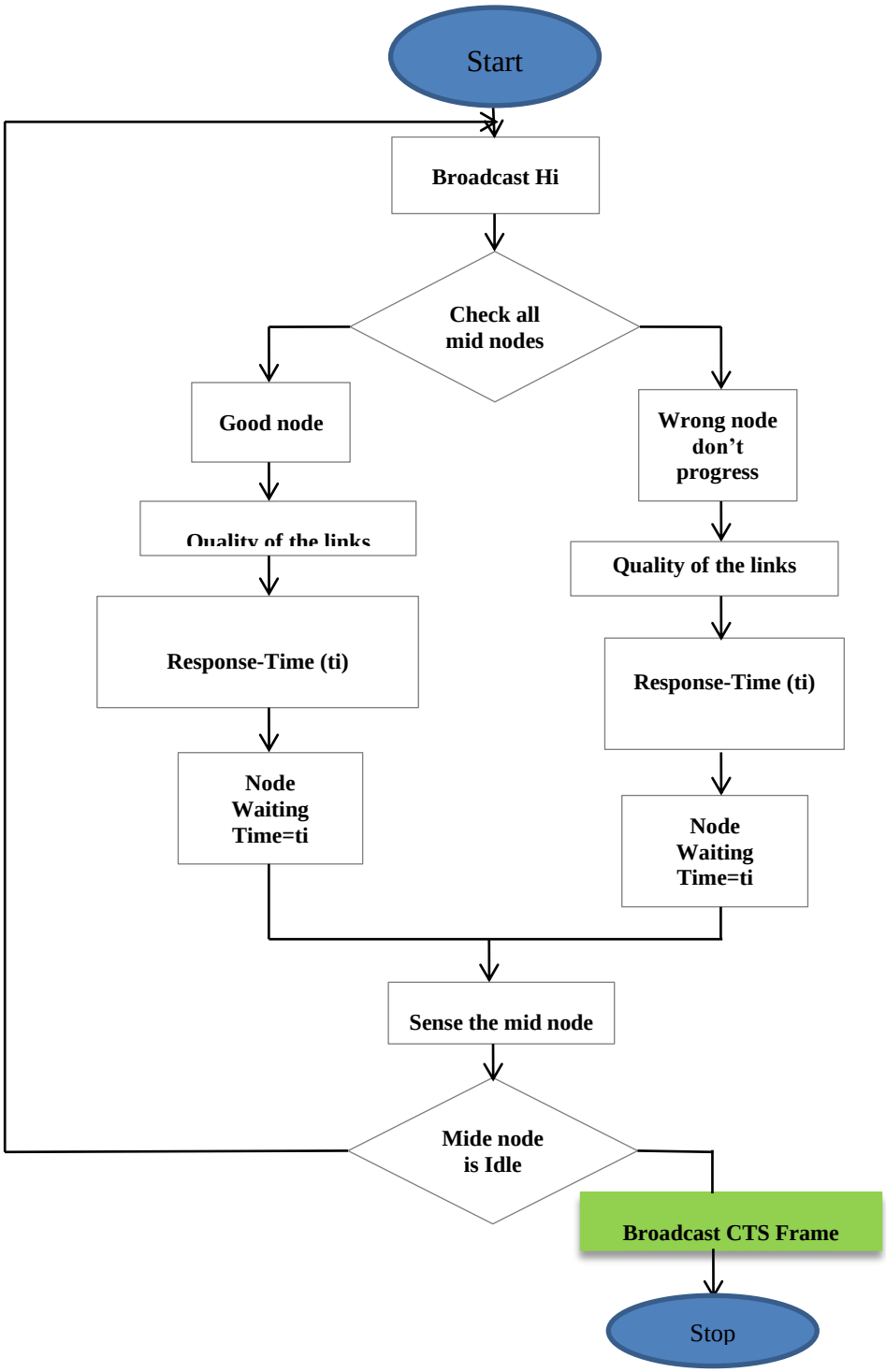

Figure-3. Functioning Of the Protocol in The Processing Nodes

The time is defined using the network allocation vector. It helps in the efficient routing of the data through the intermediate nodes. If the CTS frame reaches the source node, then the source node identifies the destination and forwards the data. If there is a network breach, and the destination node does not receive the data, then the protocol looks for breaches and solves them. In this place, a black hole attack plays a crucial role as it may cause a data breach in the network. To solve the breach and detect the black hole attack, the destination node sends a CTS frame to the source node, and the source node sends the data through the same path. The protocol adopts two methods for forwarding the data at and between intersection modules. The source node continuously tries to forward the data through the given path, and these paths are defined through the multiple-forwarding decision function (Figure-4).

The forwarded data packets carry information about both the source and destination nodes. The source node sends

the RTS frames to the router and waits until a reply comes from the router. The router plays an important role, as most malicious nodes target the router for corrupting the routing mechanism. In the router, where the protocol is implemented, the score function is calculated for the RTS frame sent by the source node if the RTS frame provides the optimal score function value.

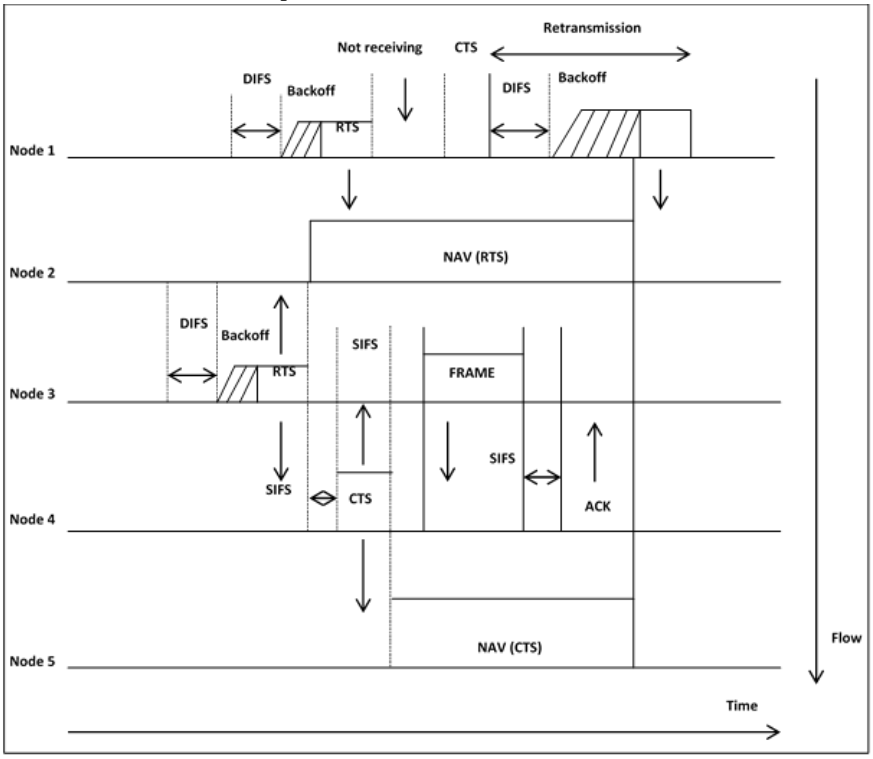

Figure-4. RTS-CTS Implementation For 5 Nodes

The data packets are forwarded to the neighboring nodes based on that optimal value. In all the RTS frames generated from the source node, the flag is the intersection identifier used to identify the intersection points in the network. It also defines whether the flag is at or between the intersection. If the node is present between the intersections, forward-to-progress gets activated, and the intersection quality is evaluated. Based on the quality of the link, the best forwarding node is selected in the network. This forwarding node is used as the intermediate node for forwarding the data. If the node is at the intersection, the greedy directional mode is activated to select the best intermediate node. Through this process, the efficient intermediate nodes are selected by the proposed mechanism for transmitting data between the source and destination. Thus, the CTS and RTS frames help evaluate the safe intermediate nodes through which the data can be transmitted. The proposed model uses the optimal score function and timer values for efficient functioning and data transmission. The communication model involves intermediate nodes in the route.

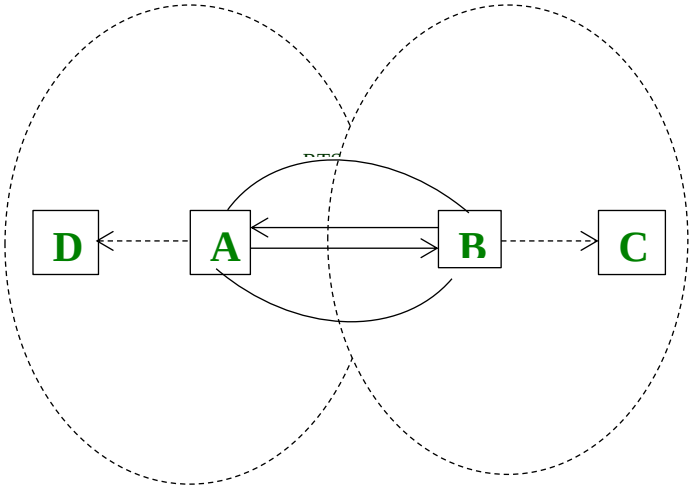

Fig-5. Example Scenario of RTS-CTS

The neighboring nodes like A, B, C, and E represent the nodes near the source node S (Figure-5). The RTS from the source node is sent to all other neighboring nodes through which the data can be transferred. The score function for all the neighboring nodes is calculated. The link quality metrics and the neighboring nodes' score function are calculated and compared to predict the nodes' weight factor. If any node has the best weight factor, and if it sends the CTS to the source, that node is self-elected. Once the node is selected, the data is transferred to the respective node. However, if the node is at the intersection point, the greedy directional approach is selected, and based on that approach, the appropriate node is selected.

Numerical model

In the proposed model, the energy consumption and throughput of the network are concentrated. The user preferences are considered through a lossy channel. Due to the collisions made in the lossy channel, the data frames are lost. Three scenarios in the collision process, like 1) collision of frames, 2) corruption of RTS, CTS, and ACK attacks, and 3) successful data transmission, are considered. The total count of nodes in the network is **n_i**, in which $\boldsymbol{i}$ represents the priority class, p_i is the probability of the busy channel,

$$\boldsymbol{p_i = b_i + (1 - b_i)p_r}$$

The possible errors and conditional collision are represented as $\boldsymbol{b_i}$ and $\boldsymbol{p_r}$. If the available nodes are busy then the data transmission among the nodes are stoped. Then, the $\boldsymbol{p_i}$ continuously changes the user priorities. The BER's average value is represented as $\boldsymbol{p_e}$, and the $p_r = 1 - (\boldsymbol{1 - p_e})^{\boldsymbol{T}}$, and in that, the payload length is represented as $\boldsymbol{T}$, which can be calculated using the following equation,

$$\boldsymbol{T = Preamble + PHY + MH + L + RTS + CTS + ACK}$$

In the above equation, the PHY represents the physical layers of the network, the MH represents the MAC header in the network, and L represents the actual data. The RTS, CTS, and ACK represent the control packets sent by them, and from that, the b_i can be expressed in the following manner,

$$\boldsymbol{b_i = 1 - (1 - \tau_i)^{n_i - 1} \prod_{j=0, j!=i}^{7} (1 - \tau_i)^{n_j}}$$

In the following process, the $\boldsymbol{\tau_i}$ represent the probable transmission of data through nodes represented in the priority classes. In the same manner, the $\boldsymbol{\tau_i}$ is calculated, which is also carried out in the previous works. The RTS and CTS packets are assumed to be transmitted through the network. The priority class $\boldsymbol{i}$ initiates values transmission in which the success of transmission and its probability is calculated through the following equation,

$$\boldsymbol{s_i = n_i \tau_i (1 - \tau_i)^{n_i - 1} \prod_{j=0, j!=i}^{7} (1 - \tau)^{n_j}}$$

The saturation throughput for the following network model is obtained from the equation,

$$\boldsymbol{s} = \frac{\boldsymbol{s_i (1 - p_{idle})(1 - p_r) T_L}}{\boldsymbol{p_{idel} \rho + (1 - p_{idle})(1 - p_s) T_c + p_s (1 - p_{idle})(1 - (1 - p_c)^r) T_s + p_s (1 - p_{idle})(1 - p_c)^r T_s}}$$

In the above equation, the $\boldsymbol{p_{idle}}$ represents the idle slot probability which can be calculated through the following equation,

$$\boldsymbol{p_{idle} = \prod_{i=0}^{7} (1 - \tau_i)^{n_i}}$$

In equation (5), if the data packet transmission is successful through a lossy channel of a priority class $\boldsymbol{i}$, then $\boldsymbol{1 - p_{idle}}$ is the exact transmission equation for the channel. The collision of the packets in the network is represented as $(\boldsymbol{1 - p_{idle}})(\boldsymbol{1 - p_s})$. The transmission error in the network is represented as the $\boldsymbol{p_s (1 - p_{idle})(1(1 - p_e)^T)}$. The slot time can be successfully transmitted through the following equation $\boldsymbol{p_s (1 - p_{idle})(1 - p_e)^T}$. The time taken for data transmission is represented as $\boldsymbol{T_L}$. The $\boldsymbol{T_c}$ represent two states both during the collision and the failure of CTS frames. The term confirms the completion of data transmission $\boldsymbol{T_s}$. To address the errors while transmitting the data packets through the network, the following equation is considered which is $\boldsymbol{p_s (1 - p_{dle})(1 - (1 - p_{es})^T) T_s}$. As the data is already transmitted, the calculations of the values like $\boldsymbol{T_c}$ and $\boldsymbol{T_s}$ need to be considered,

$$\boldsymbol{T_c = T_{RTS} + 2pSIFS + \rho + \psi}$$

$$\boldsymbol{T_s = T_H + T_{RTS} + T_{CTS} + 4pSIFS + T_{ACK} + \rho + \psi}$$

The slot time and time delay are represented as ρ and ψ. Each node awaits two iterations, one for the backoff and another for sending the RTS packet. The network's energy is wasted during the process of collisions, transmission, and errors during the channels. Hence, the overall power consumed by the network is calculated using the following equation,

$$\boldsymbol{E_i = p_{tx}\left(1 - p_i^{k+1}\right)(T_H + T_{RTS} + T_L) + P_{rx}(4pSIFS + T_{ACK}) + P_{rx} \frac{EB_i}{1 - b_i} b_i T_1 + P_{rx} \frac{p_s p_r}{(1 - p_{idle})} T_1}$$

The $\boldsymbol{k}$ and $\boldsymbol{k + 1}$ represent the initial and proceeding nodes, and their energy consumption is calculated for the successive transmissions. The $\boldsymbol{P_{tx}}$ represent the average power consumed for transmitting data, and the proposed model considered multiple power transmission levels. The

time taken for the packet to transmit through the various layers, like the preamble, header, and MAC header, is represented as $\boldsymbol{T_H}$. The power consumed at the receiving state is represented as $\boldsymbol{P_{rx}}$. The incrementation of $\boldsymbol{P_{rx}}$ is not done. If the channel is busy in the transmission process, the $\boldsymbol{E(B_i)}$ represent the mean backoff delay.

Experimental Results and Discussion

The performance of the proposed model is verified by implementing and experimenting with it with the NS2 software. The proposed RTS/CTS mechanism is implemented with the existing routing protocols to improve the performance of the VNAET in terms of end-to-end delay, PDR, packet loss rate, etc., using the NS2 simulator tool, and the input signal is simulated. The simulation process is performed on 100 nodes to find the final result. Initially, 8 nodes are examined and simulated. These 8 nodes are separated into groups A, B, and C. Groups A, B, and C comprise 3, 2, and 3 nodes, respectively. The table-1 illustrates the simulation parameter used in the proposed approach.

Table-1. Simulations Parameter

Parameters	**Value**
Packet Size	500 bytes
Simulation Time	30s
Speed of nodes (m/s)	10,15,20,25,30
Number of Nodes	8,12,16,20
Data rate	11mbps

Figure-4 represents the packet loss rate on various bandwidth values. The simulation result indicates that the packet loss value in low bandwidth is the same both with and without RTS/CTS mechanism. If the bandwidth range increases, the pack loss rate with and without RTS/CST is reduced and increased, respectively. Figure-5 indicates the end-to-end delay time of the system both with and without implementing the RTS/CST mechanism. The data transmitted using RTS/CST mechanism has transmitted the data with minimum delay time. The system without RTS/CST mechanism consumes more data transfer time. The ad hoc network system with updated RTS/CST efficiently decreases the delay time and improves the network's speed. Figure-6 indicates the average packet delivery ratio of the current and existing research work. It illustrated that the proposed protocol performs better than the existing approach [1] when the number of nodes increases. That is. The PDR ratio is effectively balanced and increases when the number of nodes reaches 300. But the PDR ratio of the existing model decreases when the node increases.

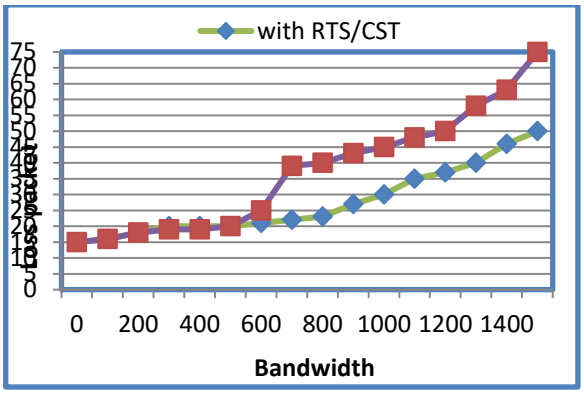

Figure-4. Packet Loss Ration with And Without RTS/CST Mechanism

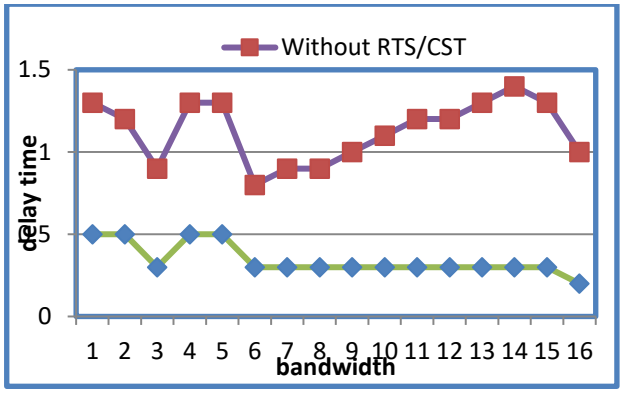

Fig-5. Delay Time with And Without RTS/CST Mechanism

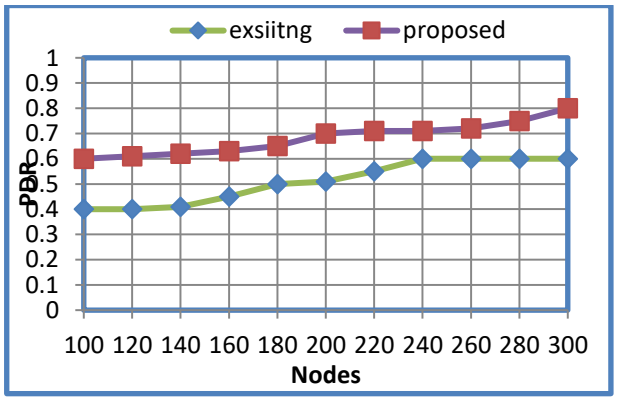

Figure-6. PDR Comparison

Figure-7 graphically depicts the average delay time of the present and existing approaches. It shows that the proposed routing protocol performs better compared to the existing approach. It also clearly indicates that the delay time in the proposed model decreases when the number of nodes increases. At the same time, the existing approaches have consumed more time when the number of nodes increases to transmit the data. The overall result of the proposed routing protocol illustrates that it performs better than the other existing approaches and accurately transmits the data between the nodes without any packet loss.

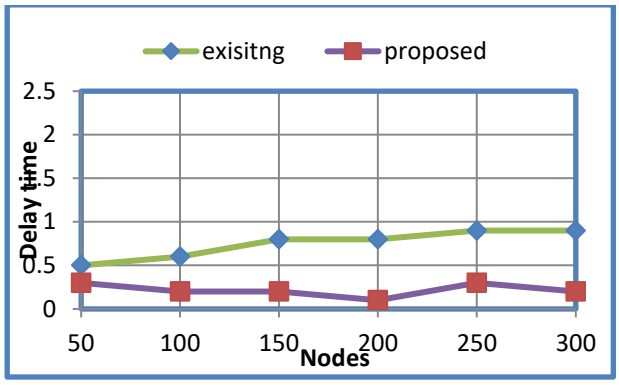

Fig-7. Average delay time of the proposed and existing approach.

Table-4.3 shows the performance metrics of the proposed algorithm in terms of the number of Nodes, throughput, PDR, Remaining energy, and Packet loss. The network's throughput is much higher, and it is easy for the network to handle the data and efficiently use the available bandwidth. The packet delivery ratio of the network is also consistent, and due to this, the network is consistent in performance; also, the packet loss of the network is negligible compared to PDR. The network's energy consumption is also much less due to the network's optimized functioning and the data's routing. It should also be noted that with the increased number of nodes, all the parameters are consistent and increasing, thus providing a better WSN model. From the above table, the proposed hybrid MAC-PDMA-based optimization provides better efficiency to the network. It should also be noted that the network is providing better performance regarding various QoS factors.

This paper proposed an RTS-CTS mechanism for detecting blackhole attacks in the network. The packet forwarding protocol uses the RTS and CTS frames to detect the network's blackhole attacks. The protocol detects the blackhole regions and routes the data through different paths. This routing helps in escaping from such attacks. The mechanism of detecting blackhole regions is discussed in the paper. The proposed network is simulated in NS2, and the network parameters are considered to evaluate the performance of the proposed network. A numerical model is generated, which detects the RTS, CTS, and ACK attacks that form the root cause for the black hole attacks.

Table-4.3. Performance Evaluation

No. of nodes	Throughput	PDR	Remaining Energy	Packet loss
50	1843	1.00	98.64	0
100	2942	0.98	98.16	0.02
150	3678	0.97	97.55	0.03
200	4453	0.975	96.78	0.03
250	4907	0.973	96.35	0.03
300	5611	0.982	95.68	0.02
350	6210	0.972	94.98	0.04
400	6812	0.975	93.98	0.03
450	7400	0.969	93.36	0.03
500	8032	0.975	93.18	0.03

Conclusion

The proposed model calculates the probability of a blackhole attack in the network through the network's networking parameters and power consumption. Based on the functioning of the node in the network, malicious nodes are evaluated, and the black hole region is found. The proposed model is simulated in NS2 software, and the results are compared with an existing algorithm. The comparison shows us that the proposed algorithm performs better regarding network throughput, PDR, and delay time.

In future works, the scalability of the network can be increased, and blackhole attack detection ratio verified using Machine learning algorithms.

References

[1] Dhaka, A., Nandal, A., & Dhaka, R. S. (2015). Gray and black hole attack identification using control packets in MANETs. *Procedia Computer Science*, *54*, 83-91.

[2] 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.

[3] Naveena, S., Senthilkumar, C., & Manikandan, T. (2020, March). Analysis and countermeasures of blackhole attack in manet by employing trust-based routing. In *2020 6th international conference on advanced computing and communication systems (ICACCS)* (pp. 1222-1227). IEEE.

[4] Choudhury, D. R., Ragha, L., & Marathe, N. (2015). Implementing and improving the performance of AODV by receive reply method and securing it from Black hole attack. *Procedia Computer Science*, *45*, 564-570.

[5] Srinivasan, V. (2021). Detection of Black Hole Attack Using Honeypot Agent-Based Scheme with Deep Learning Technique on MANET. *Ingénierie des Systèmes d'Information*, *26*(6).

[6] Rani, P., Verma, S., & Nguyen, G. N. (2020). Mitigation of black hole and gray hole attack using swarm inspired algorithm with artificial neural network. *IEEE Access*, *8*, 121755-121764.

[7] Moudni, H., Er-rouidi, M., Mouncif, H., & El Hadadi, B. (2019). Black hole attack detection using fuzzy based intrusion detection systems in MANET. *Procedia Computer Science*, *151*, 1176-1181.

[8] Thanuja, R., & Umamakeswari, A. (2019). Black hole detection using evolutionary algorithm for IDS/IPS in MANETs. *cluster computing*, *22*(2), 3131-3143.

[9] Pandey, S., & Singh, V. (2020, July). Blackhole attack detection using machine learning approach on MANET. In *2020 International Conference on Electronics and Sustainable Communication Systems (ICESC)* (pp. 797-802). IEEE.

[10] Farahani, G. (2021). Black hole attack detection using K-nearest neighbor algorithm and reputation calculation in mobile ad hoc networks. *Security and Communication Networks*, *2021*.

[11] Joseph, C., Kishoreraja, P. C., Baskar, R., & Reji, M. (2015). Performance evaluation of MANETS under black hole attack for different network scenarios. *Indian Journal of Science and Technology*, *8*(29), 1-10.

[12] Yadav, S., Trivedi, M. C., Singh, V. K., & Kolhe, M. L. (2017, October). Securing AODV routing protocol against black hole attack in MANET using outlier detection scheme. In *2017 4th IEEE Uttar Pradesh Section International Conference on Electrical, Computer and Electronics (UPCON)* (pp. 1-4). IEEE.

[13] Mahin, S. H., Taranum, F., Fatima, L. N., & Khan, K. U. (2019). Detection and interception of black hole attack with justification using anomaly based intrusion detection system in MANETs. *International Journal of Recent Technology and Engineering*, *8*(11), 2392-2398.

[14] Keerthika, V., & Malarvizhi, N. (2019). Mitigate black hole attack using hybrid bee optimized weighted trust with 2-Opt AODV in MANET. *Wireless Personal Communications*, *106*(2), 621-632.

[15] Eid, M. M., & Hikal, N. A. (2021). Enhanced Technique for Detecting Active and Passive Blackhole Attacks in MANET. In *Proceedings of the International Conference on Advanced Intelligent Systems and Informatics 2020* (pp. 247-260). Springer International Publishing.

[16] Moudni, H., Er-Rouidi, M., Mouncif, H., & El Hadadi, B. (2018). Fuzzy logic based intrusion detection system against black hole attack in mobile ad hoc networks. *International Journal of Communication Networks and Information Security*, *10*(2), 366-373.

[17] Khan, D. M., Aslam, T., Akhtar, N., Qadri, S., Rabbani, I. M., & Aslam, M. (2020). Black hole attack prevention in mobile ad-hoc network (manet) using ant colony optimization technique. *Information Technology and Control*, *49*(3), 308-319.

[18] Yasin, M. B., Khamayseh, Y. M., & AbuJazoh, M. (2016). Feature Selection for Black Hole Attacks. *J. Univers. Comput. Sci.*, *22*(4), 521-536.

[19] Nagalakshmi, T. J., Gnanasekar, A. K., Ramkumar, G., & Sabarivani, A. (2021). Machine learning models to detect the blackhole attack in wireless adhoc network. *Materials Today: Proceedings*, *47*, 235-239.

[20] Hikal, N. A., Shams, M. Y., Salem, H., & Eid, M. M. (2021). Detection of blackhole attacks in MANET using adaboost support vector machine. *Journal of Intelligent & Fuzzy Systems*, (Preprint), 1-14.