International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2024/224433 Volume 11, Issue 1, January – February (2024)

RESEARCH ARTICLE

Co-Ordinated Blackhole and Grayhole Attack Detection Using Smart & Secure Ad Hoc On-Demand Distance Vector Routing Protocol in MANETs

Sampada H K
Department of Electronics and Communication Engineering, Atria Institute of Technology, Bangalore, India.
sampada.hk@atria.edu

Shobha K R
Department of Electronics and Telecommunication Engineering, Ramaiah Institute of Technology, Bangalore, India.
shobha_shankar@msrit.edu

Received: 08 August 2023 / Revised: 04 January 2024 / Accepted: 21 January 2024 / Published: 26 February 2024

Abstract – Mobile Ad Hoc Network (MANET) devices are powered from battery and due to infrastructure-less feature, the security and energy consumption are major concerns. Most of the researchers have assumed that the Cluster Head (CH) nodes are benign and frequently undergo cluster re-election, which shortens the network lifetime. Smart & Secure Ad Hoc On-Demand Distance Vector algorithm (S^2-AODV) is proposed with secondary CH (S-CH), primary CH (P-CH) and a super cluster head (SCH) node along with the other nodes. Modified-AODV (M-AODV) is used for neighbor discovery. Weight-based clustering algorithm is proposed, with the primary and a secondary CH node to enhance the network efficiency. S^2-AODV enhances security using Honey-pot AODV (H-AODV) and avoids the CH re-election process enhancing the overall network lifetime. The proposed algorithm works in off-line mode and on-line mode. In off-line mode the various Wi-Fi parameters like Received Signal Strength Indicator (RSSI), transmission power, battery level, distance and number of transmissions retries are collected from each CH node in the network. A look-up table indicating the transmission power (TXP) to be set by the CH nodes is determined by machine learning (ML) algorithms. This table is circulated among every CH node by SCH node in the network. Due to this process the intermittent reelection of the P-CH and S-CH nodes can be avoided, enhancing the network lifetime. In on-line mode, SCH executes H-AODV to identify and remove the malicious CH (black hole / gray hole) nodes (ns-2.34).

Index Terms – MANETs, AODV, M-AODV, H-AODV, Cluster, Black Hole Attack.

1. INTRODUCTION

MANETs are self-reliant infrastructure-less networks. They are simple to set up but extremely challenging to maintain. Since MANET devices run on batteries, two of their biggest issues are security and energy consumption. These networks also suffer from a lack of infrastructure. Due to dynamic nature of the nodes in MANET [1][2][3][4] and as entire network relies on battery, nodes become weak sometimes and take a long time to replenish or recharge, which poses a significant challenge. Depending on the circumstance, batteries or substantial electrical power sources are used to power the nodes in an Ad Hoc system. Energy usage depends on packet delivery when the wireless port on a cell node is off, which happens when the device is inactive or asleep. Worries about the amount of energy lost as a result have given room for researchers to work in this domain. Since they are portable, mobile Ad Hoc system devices require mobility. Despite improvements in technology for extending battery life, a substantial barrier to the widespread usage of battery-operated gadgets has been sustained. Researchers to get around this challenge, need efficient protocol, platform, and technological design are needed. They are none the less limited in terms of weight, size, and resource availability in terms of bandwidth and battery capacity [5][6]. As a result, the energy efficiency of MANETs continues to be a key design element [7]. Similar to other communication systems based on radio, MANETs are susceptible to a number of threats. The threats can be from both internal and external attackers. To safeguard these systems from cyberattacks, a range of solutions for information assurance, such as identity management, access control, and data protection are adopted [8] [9]. Among the most typical methods by which nodes lose energy is because of communication [10][11][12]and mobility. The nodes must become less mobile to improve the battery capacity. Security being another major issue in MANETs as the nodes are computationally not very strong.

As a result, MANET energy efficiency and security is still a crucial component of their design. To protect these systems, a range of information assurance measures, such as identity management, access control, and data protection, will need to be put in place from attacks [13][14]. Blackhole and grayhole attacks are the most dangerous attacks as they disrupt the network by reducing the resources.

In order to enhance security in MANETs, a more decentralized approach called Clustering can be implemented. Clustering is the process of restructuring the entire network into smaller networks. In MANETS, clustering provides various benefits like security, load balancing resource management to name a few, over other types of networks. A certain node is elected to serve as the Cluster Head (CH) based on a certain criterion or just randomly. Some of the criteria are a node's ID, weight, degree of mobility, etc. The CH and the nodes within the group exchange information. As a result of communication between cluster heads, unwanted traffic flow is reduced in the network. Cluster Gateways facilitate communication with neighboring clusters. Therefore, a cluster head, gateways, and member nodes make up each and every cluster. By enhancing efficiency and lowering the possibility of interference, clustering in MANET improves network QoS parameters like throughput, latency, lifetime, security etc. MANETs are vulnerable to a variety of network layer assaults because there is no centralized mechanism available. Sybil Attacks, Byzantine, Worm Hole, Black Hole, and Gray Hole are a few types of network layer attacks that degrade networks and cause data loss by destroying the topology of the network [15][16][17]. A node promises to have the shortest pathways to every destination in the Black Hole Attack [18]. Utilizing the routing protocol, this node consumes all network data packets, reducing network performance. Hence proposed work mainly addresses energy and security issues in MANETs, using S^2-AODV protocol. Weight based clustering is used with the addition of super CH, P-CH and S-CH. Few ML algorithms are also implemented to fix the transmitted power of CH nodes.

The work's primary contributions are listed below:

- Mathematical model (AHP) based; Weight-based CH selection technique is implemented. Based on the maximum weight among the different CH nodes in the network, P-CH, S-CH, and Super Cluster Head (SCH) are elected. AHP mathematical model is used as the weight of a node is dependent on multiple parameters like trust, constancy and no. of neighbors in the network.
- Smart AODV (energy efficient and secure) which works in 2 modes:

S^2-AODV (off-line mode): Utilize lookup tables generated from machine learning methods such as Random Forest, Decision Trees, and SVM and Naive Bayes to optimize the transmission power of the CH nodes and thereby preserve the network battery life. 92% efficiency was the highest given by Random Forest. SCH node distributes the look-up table to CH nodes in order to set their TXP and improve network battery efficiency and enhance the lifetime

S^2-AODV (on-line mode): Usually CH nodes are considered to be authentic nodes which may not be true in all cases. Hence in this approach SCH and CH nodes execute H-AODV to identify and remove the coordinated malicious the network's nodes.

S^2-AODV, M-AODV, and H-AODV are compared with the existing AODV and C-SSA using different mobility and propagation models. Regarding latency, throughput, network lifetime, and detection rate, S2-AODV performs better.

The rest of the document is structured as follows: In section 2, the related works are displayed. Section 3 explanation of the proposed algorithm. In Section 4, the outcomes of the recommended method are provided along with a thorough analysis. Section 5 offers a summary of the completed work.

2. LITERATURE REVIEW

MANETs are highly vulnerable networks because of their decentralized nature. Node battery is a prime concern as the nodes are mobile. Many researchers are working to enhance the security and network lifetime in MANETs [19] [20]. Clustering helps to make the network more scalable and helps in deploying the algorithms for security. Mobility models and propagation models also affect the performance of MANETs to a large extent [21] [22]. Veeraiah et al. [23] presented C-SSA algorithm for navigation that is both safe and energy-efficient, based on node trust. Principal goal of the project is to decrease the energy loss in the network during transmission. It is a hybrid optimization technique working in three parts. It employs a fuzzy hybrid clustering technique using trusts in Direct (DT) and Indirect (IDT) Forms and Recent Trust (RT). Direct trust is the record of the communication between the ith node and jth node for a certain period involving the public key technique. Indirect trust is calculated between the nodes using a witness node between ‘i’ and ‘j’ nodes. Recent trust is calculated by the destination node considering both DT and IDT with an extra variable called validity. A node is considered malicious if the total trust value falls below 0.5J. The best route between source node (SN) and destination node (DN) is calculated using a hybrid algorithm called Cat Slap Optimization (CSO) and Slap Swarm Optimization (SSA). The C-SSA which is a combination of CSO and SSA choses the best path between SN and DN using a fitness function involving remaining energy, throughput and connectivity. The CHs participate when routing in multiple hops in line with the suggested hybrid protocol, where the best route is chosen by analyzing the connectivity, throughput, and latency. Energy usage, throughput, and rate of detection are in contrast to the current techniques and C-SSA performs better. Algorithm works well only for single attackers and not for multiple attackers. In order to improve security in Protocol for Ad Hoc on-Demand Vectors (AODV) additionally other reactive routing guidelines, Anantapur and Patil [24] suggest a hash function method. AODV routing technology is used to move packets of data from one place to another. Utilizing a hash function with location updates to prevent selfish nodes approach is strongly advised to minimize packet loss over the network as a whole. Though the algorithm is complex due to the use of Hash function it is energy efficient and secure. A new and effective data transfer approach with an encryption-based approach has been presented by Rajashanthi et.al.,[25]. Grey Wolf Optimization Adaptive Formation (GWOAF) to optimize adaptive network formation has been proposed in this work. A new encryption technique called homomorphic is used to pick the best route from the available options for protecting data key management techniques. Results are compared with safe routing system based on trust based on the atom whale optimization algorithm through the application of the trust-aware routing protocol. It uses end-to-end latency, PDR etc. as QoS parameters.

Nithya et al. [26] present a fuzzy but security-conscious method for ant colony routing optimization. In typical common states of attack and scenario, any network routing protocol should be able to offer a consistent ratio of packet transfers, reduction in latency and connection overhead. The enhanced fuzzy algorithm atom whale Algorithm for Optimization (AWOA) [27] was used to build the routing organization, which is an improvement over AODV. Millimeter-wavelengths are required for millimeter-wave to play an important function in 5G, so this study is focused on assessing the potential effectiveness of a MANET using Millimeter Wave equipment. MANETs reduced packet transmission loss using mm Wave, resulting in better Signal to Noise Ratio and enhanced performance.

Alappatt and Prathap suggest a routing strategy that is energy-efficient [28]. To choose the secure multipath routing, sequence numbers are used in order to locate and separate the susceptible nodes in the network. The packets of data are protected from data transfer attacks using Hybrid Honey Encryption (SH2E), a secret key-centered method. The optimal path is determined from the selected multipath using the Shuffled Shepherd Optimization (LF-SSO) algorithm developed by Levy Flight Centered. This method employs a route determined by residual energy, trust and path distance in order to increase the network's longevity. Before broadcasting to the base station, decrypted data packets are transferred from the SN to the DN via the most efficient route. This effort takes route maintenance into account in addition to energy-efficient secure routing. The PDR is increased by the LF-SSO to 0.89, and the TNL (network lifetime) is increased to 437 hours. The SH2E method, in contrast, takes just 4176 milliseconds to encrypt the 50kb DP (data packets) and achieves a security level of 98.54%.

K. K. Thangadorai *et al.*, [29] proposed an Intelligent Mobile Hot Spot Power Save (I-MHSPS) technique based on Machine Learning (ML) that uses Wi-Fi characteristics like RSSI, SNR, TXP (transmission power) and link state. Intelligent Transmit Power Control (I-TPC): uses SVM ML algorithm to learn the suggested TXP for the MHS (mobile hot spots). It uses 8 different classes to categorize the data based on the RSSI (received signal strength indicator), total retries, transmission rate. I-MHSPS utilizes the MHS State Machine over the Android foundation. To store the aforementioned statistics, MHS Manager immediately communicates with the database manager after receiving input from the user battery Statistics Manager, Wi-Fi Core Manager, and Wi-Fi Scan Manager are additional modules that help with data gathering. The connected Station (STA) data, which is obtained from the Wi-Fi driver, as well as other Wi-Fi environmental variables, are provided by the Wi-Fi core manager. The Wi-Fi scan manager lists all additional networks that are close their BSS loads to MHS. The device's battery load, remaining power, and charging state are all provided by the battery statistics manager. MHS Manager and the model trained using SVM provide information to the Power Save Manager, which controls the MHS TX power.

Intelligent Low Power Encryption (I-LPE) module is where the choice is made whether to activate low-power encryption to lower MHS power usage. The I-TPC module sends a signal after the main TPC mechanism has been activated. LPE collaborates closely to lower security threats. I-LPE calculates the device's proximity using several Core Wi-Fi Manager Factors Core LPE is triggered if the device is close enough to the MHS. This, along with the core TPC algorithm, greatly lowers power consumption. Mobile phone notification panels are used by the Intelligent Ultra Power Save (I-UPS) recommendation engine and low power encryption for short range MHS to notify users of their device's remaining battery life. This will further help users to put the mobile phone in power save mode MHS will start consuming battery more quickly as soon as the user switches it on. Statistics on battery usage result in finding the usage trend and help in predicting the battery usage of the user. Based on the various applications that users may use frequently like, time of day, weather forecast application etc.

Prediction of the next application provides information regarding the usage of data behavior, including whether the application consumes information or not. To reduce power usage, the user can be advised to enable UPS based on this behavior. Applying various system power levels for MHS operation the I-TPC concept lowered power consumption by roughly 10–16% compared to conventional methods. Results indicate a significant decrease in MHS power usage without a noticeable performance penalty. Jie Gu et al. [30] explains intrusion detection based on Support Vector Machine (SVM) and Naive Bayes' feature embedding. The Naive Bayes feature transformation method is applied to produce new, high-quality data from the original features. An SVM classifier is trained with the transformed data, and the resulting intrusion detection model is produced. Experiments conducted on various datasets within the intrusion detection domain have demonstrated the good and robust performances that can be achieved by the proposed detection method. The accuracy of this method on the Kyoto 2006+ dataset was 93.75%. The accuracy, detection rate, and false alarm rate of the method are its main advantages. Routing is a significant problem in networks regardless of the environment being wired or wireless [31].

Routing is very challenging in MANETs, which are adaptable and decentralized wireless networks. Additionally, malicious nodes present in the MANET can harm the transit system. network effectiveness. Reinforcement learning has recently been suggested as a solution to these issues. The Q-learning mechanism, which is a reinforcement learning algorithm, is appropriate for an opportunistic routing strategy because it not only adapts to shifting networks but also lessens the impact of malicious nodes on packet transmission. In this study, a reputation opportunistic routing, a new reinforcement learning routing protocol for MANETs is built on Q-learning. (RORQ). This protocol is based on game theory and enables efficient routing, allowing a reputation system to detect and block malicious nodes in a network. More than other state-of-the-art routing techniques, the method can find a routing route more successfully in a malicious node environment. Furthermore, the proposed method demonstrated improvements of up to 73% in packet loss, up to 35% in average end-to-end delay, and up to 12% in energy efficiency in the case of a gray hole attack, and up to 55% in packet loss, up to 82% in average end-to-end delay, and up to 28% in energy efficiency when compared to other algorithms that were used.

The dynamic character of the MANET makes it vulnerable to energy and security restrictions. Energy optimization is a difficult problem for most of the techniques, but it is successfully solved by routing protocols. Considering this, an effective multipath routing protocol for MANET built on an optimization algorithm [32] was put forth. The MANET's energy and security crisis is effectively handled by the cluster head (CH) selection and intrusion detection techniques, namely fuzzy clustering and fuzzy Naive Bayes (fuzzy NB). Then, using safe nodes, the bird swarm-whale optimization algorithm (BSWOA), which combines the whale optimization algorithm (WOA) and the bird swarm optimization algorithm (BSA), is used to advance multipath routing. The optimal paths are selected based on fitness variables such as throughput, energy, trust, and connectivity. Based on performance metrics, the techniques are examined using attacks like flooding, blackholes, and selective packet drops. In the presence of the attack, the suggested BSWOA obtained the maximum energy, minimum delay of 0.00372 ms, 0.676 bps, 69.9%, and detection rate, and throughput of 9.48 Joule, respectively. An innovative method for the millimeter frequency band [33] in interior situations stairway is proposed. The two signals in this work were considered to measure the two stairwells. The strategy can prompt an instant reaction when the siren is activated for emergency purposes. The directional siren antenna is set up with the range of 26, 28, 32, and 38 GHz for both co-polarization and cross-polarization at various millimeter frequencies. For the investigation and analysis, four distinct radio wave route loss propagation models have been employed. Reference models for near in free space and floating intercept path loss have been implemented. The alpha, beta, gamma, and frequency dependent path loss are used to analyze the different frequencies. The efficacy of the multi-floor stairwell's signal strength is found to be beneficial for examining path loss. Similar results are obtained for standard deviations, path loss exponent values, and other metrics.

In [34] and [35], authors put forth a Ray Tracing (RT) model named channel to investigate the effects that realistic localization systems can have on wave propagation. The testing is conducted from this perspective using 3-D data from a hypothetical university campus. The channel impulse response (CIR) stimulus is tested via the RT utilizing a variety of propagation techniques and mechanisms. The Mobile Ad Hoc network's performance is severely constrained due to mobile radio channels [36]. The node itself collaborates with other devices to coordinate and control the network since these networks run without the need for any infrastructure or centralized control. The rate at which a signal fades as a node moves through space depends on how prompt the signal is. With the use of several scenarios and propagation models, including free space, two-ray ground, and shadowing, the performance of the Ad Hoc On-Demand distance vector Routing (AODV) protocol for MANETs with channel fading is to be assessed in this study. The performance of the Ad Hoc on-demand distance vector (AODV) routing algorithm has been investigated for two distinct fading patterns, which are typical of urban environments and include Rayleigh and Lognormal Shadowing.

The effects of four different mobility models—Gauss Markov (GM), Manhattan Grid (MG), Random Waypoint (RWP) [37], Reference Point Group Mobility (RPGM), and varying node density—have been taken into account. The results show that AODV performance for the tested cases is significantly worse for slow fading (also called Lognormal Shadowing) channel than for fast fading. The effectiveness of AODV is highest when the nodes tend to cluster (i.e., with RPGM), but it is particularly poor for both GM and MG models. When the nodes are further apart, for example In MANETs, the Trust Based AODV (TAODV) [38] routing protocol aids in the identification and elimination of black hole attacks. Because BH nodes increase network overhead and interfere with regular network operation, they pose a serious security risk. Mobile Ad Hoc networks relay information between nodes through connections. At creation, every node has a 0.7 trust rating. A source node sends a packet to its neighbors, who subsequently forward it to the target nodes in order to request a route. If the route is found, the intermediate node sends the same route request to its neighbors, who in turn forward to other intermediate nodes until the destination is found. If the route is not found, the neighbor node searches for it first in its cache memory and sends a route reply to the source node. When a route reply communication from the neighboring nodes is received the source node examines the replying nodes' sequence numbers and trust indices first, then chooses the node with the best reputation to relay messages. The chosen neighbour nodes are used to transmit the information from the source node. A neighbor becomes more trustworthy when a communication is delivered well. If the promise is broken, the value of the trust declines. "Black hole nodes" are all nodes that have a trust score of less than 0.7 and are blocked from access.

This investigation uses TAODV, which can be applied to a variety of traffic patterns, such as Pareto, Exponential, and CBR. As a propagation environment, indoor shadowing environments are used to observe different service quality levels (QoS). The Trust based AODV (TAODV) routing protocol is presented in this paper to reduce the impact of a Black Hole attack. To optimize packet delivery ratio and throughput, exponential traffic conditions are favored when a node's mobility is based on the Gauss-Markov mobility model for indoor environments. However, exponential traffic conditions are preferred to achieve the best results in terms of packet delivery ratio and throughput if a node's mobility is based on the Random walk mobility model.

Most recent results in Mobile Ad Hoc Networking have been obtained utilizing simulators [39]. Tools for network simulation are commonly used to evaluate how well MANET protocols and applications perform. The use of real-world measurements for such kinds of networks is constrained by the requirement for repeatable results and easily observable settings. They usually provide basic radio propagation models, which ignore environmental impediments. The radio wave propagation model has a major impact on the simulation results. Here, it is asserted that the two more accurate radio propagation models—the free-space propagation model and the two-ray ground model—have a major impact on the simulation results. The urban simulation region's data serves as the foundation for the model. Different conclusions from performance evaluations are therefore anticipated. This paper presents the results and parameters of the simulation, as well as the influence of these MANET propagation models in indoor and outdoor environments. This study examines the performance of the AODV, AOMDV, DSDV, and DSR protocols from the perspectives of three different propagation models: two-ray ground, shadow, and free space model. Two separate scenarios are used to evaluate the simulation's performance, and the 95 percentile findings are shown while taking nine replications into account. The findings show that protocols have kept their fundamental properties across many contexts, albeit with considerable differences when the influence of various propagation models is considered.

MANETs propagation models use a variety of communication scenarios [40], such as direct Line of Sight (LoS), Non-Line of Sight (N-LoS), two-ray ground reflection, etc. These propagation models face issues like separation due to communication, which directly affects how effective they are. This article has used two-ray ground and free-space radio wave propagation models to analyze the distance-based scenarios in different distance ranges. NS-2 simulations have been conducted using average throughput, average latency, and average packet drop as performance evaluation metrics. The simulations demonstrated that distance has a direct effect on propagation models' efficacy. It finds that the two ray ground model performs at the highest level when compared to the free space propagation model. The primary reason is two-ray ground's use of two-way ground reflection for LOS and N-LOS communication. The distance-based scenario used to evaluate the efficacy of the AODV routing scheme is significantly impacted by the suggested radio wave propagation models, as per the simulation results.

2.1. Working of C-SSA Algorithm

Results of S^2-AODV is compared with C-SSA algorithm and it is explained in detail below. C-SSA [25] as shown in figure 1, uses a hybrid routing mechanism that is trust-aware, safe and energy-efficient. In order to reduce transmission-related energy loss and lengthen the system's lifetime, the research also presents an algorithm that is hybrid that combines the Cat Slap Optimization (CSO) and Slap Swarm Optimization (SSA) algorithms. Using the maximum values of direct, indirect, and recent confidence, the first step involves choosing a CH and performing fuzzy clustering. The second step uses a predefined threshold value of 0.5J to identify intruded nodes. If a node's trust value exceeds this threshold, it is categorized as regular; otherwise, it is categorized as an intruded node. By doing this, we safeguard the node from intrusion and ensure that secure data is transferred from the source to the destination. The suggested hybrid C-SSA algorithm, which is based on the intended target feature and considers the path's capacity, throughput, and communication, is then used to select the best paths. The hybrid optimization-based, safe, energy-efficient, trust-conscious routing in MANETs. The three trust values that are employed are recent trust (RT), indirect trust (IDT), and direct trust (DT). The average of the three trust values is used to choose the CH node. Between the nodes is DT. IDT originates from an Intermediate Node (IN) node, and the basis for recent trust is the nodes' most recent exchange of messages. Throughput, energy consumption, and detection rate are contrasted with the methods currently in use.

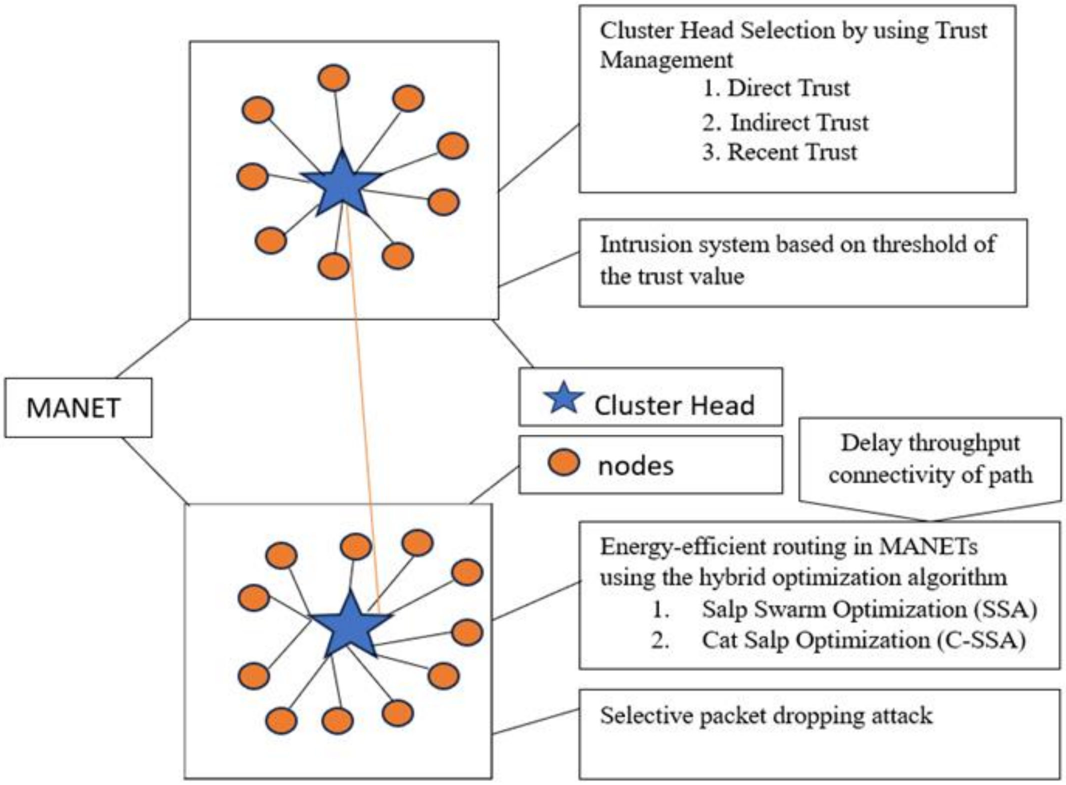
Cluster Head Selection by using Trust Management
1. Direct Trust
2. Indirect Trust
3. Recent Trust
Intrusion system based on threshold of the trust value
MANET
Cluster Head
nodes
Delay throughput connectivity of path
Energy-efficient routing in MANETs using the hybrid optimization algorithm
1. Salp Swarm Optimization (SSA)
2. Cat Salp Optimization (C-SSA)
Selective packet dropping attack

Figure 1 Cat Slap Single-Player Algorithm (C-SSA)

2.2. Problem Statement

To detect and avoid Co-ordinated attacks from multiple malicious Nodes in Manets & ensure packet forwarding.

3. METHODOLOGY

The development of an intelligent and secure routing algorithm for MANET is the main goal of this approach. For normalizing the node's battery. Various ML algorithms are used. Several secure iterative routing methods dependent on intrusion node identification and CH selection mechanisms for energy efficiency and security. Weight based CH selection techniques are easy and efficient. For effective and observable routing, the intruded node is detected using the baiting approach.

A novel weight-based CH selection technique with highest values of stability, trust, and maximum neighbors is considered. Subsequently, a novel node named SCH initiates an intrusion detection protocol to identify intruding CH nodes and guarantee the dependable their packets' transfer from the source to the destination. CH nodes will perform H-AODV to detect and remove CBH / CGH nodes from their network. Transmission power of the CH nodes is normalized using various ML algorithms to ensure cluster re-election avoidance by having a primary CH (P-CH) and secondary CH (Se-CH). So, a SCH, P-CH and Se-CH are used in the network for effective maintenance of cluster and avoidance of security threats.

The network QoS parameters are impacted by random mobility models include random direction, random walk, and random waypoint. Propagation models like the two-ray ground model, free space model, and shadowing model also affect the network performance. A combination of these parameters is assessed for S^2-AODV and compared with AODV, M-AODV, H-AODV, C-SSA. Performance of S^2-

AODV was found to be better for QoS parameters and network scalability.

In order to reduce cooperative BH/GH attacks, S2-AODV (Figure 2) improves on M-AODV and H-AODV and incorporates machine learning (ML) algorithm inputs. It does this by increasing the energy efficiency of the clustered environment.

- By having a primary and secondary CH, avoiding CH re-election, and optimizing the transmission power of the CH using a variety of ML algorithms, the network's energy efficiency is increased. SCH node is introduced to keep an eye on CH node misbehavior. In order to reduce battery consumption, SCH sends the look-up table to every CH node, allowing the TXP to be adjusted appropriately.
- The network's security is enhanced by the SCH node's use of the H-AODV algorithm to eliminate malicious CH nodes (posing as BH / GH nodes). Consequently, raising the QoS metrics.

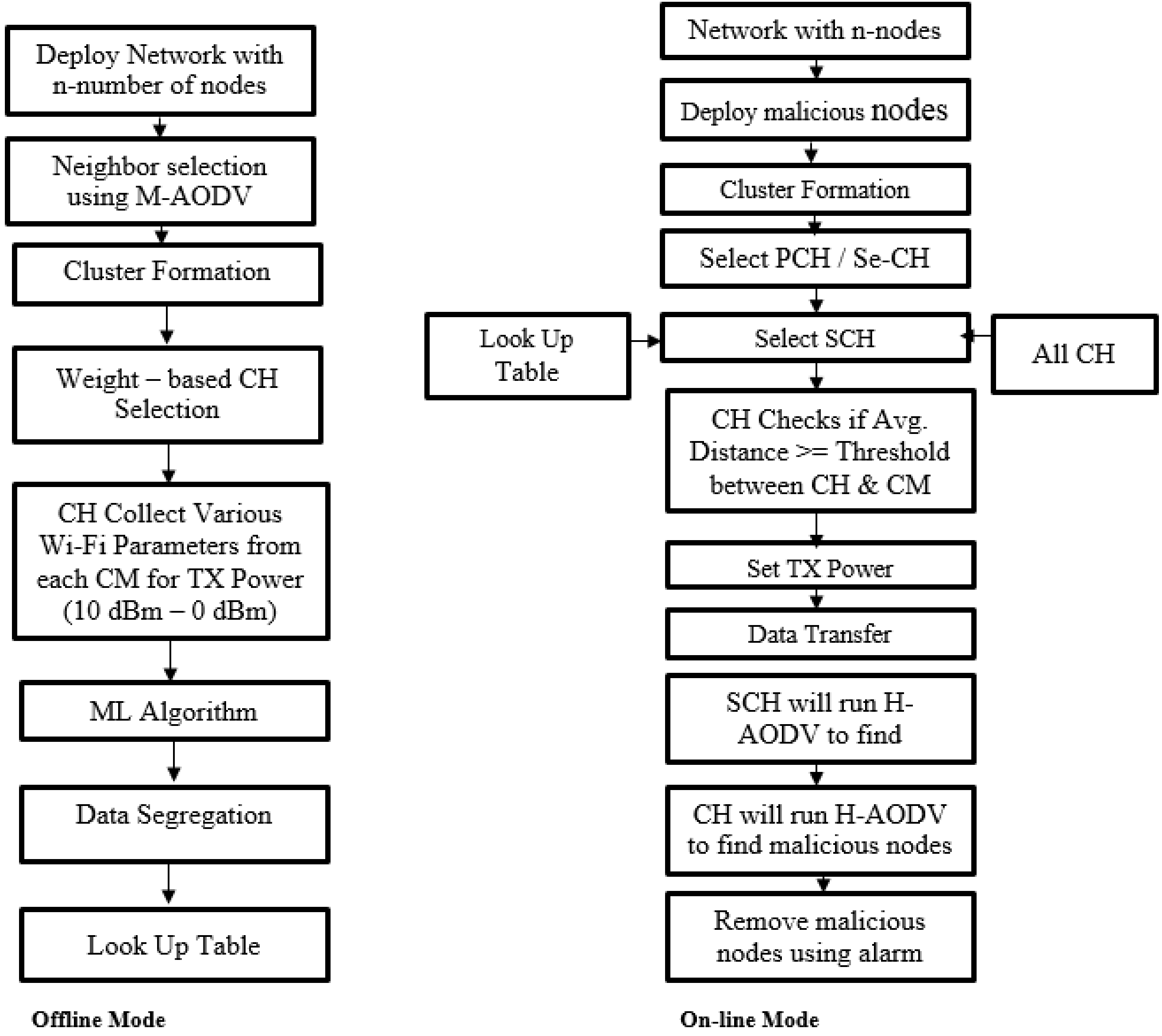
Deploy Network with n-number of nodes
Neighbor selection using M-AODV
Cluster Formation
Weight – based CH Selection
CH Collect Various Wi-Fi Parameters from each CM for TX Power (10 dBm – 0 dBm)
ML Algorithm
Data Segregation
Look Up Table
Offline Mode
Network with n-nodes
Deploy malicious nodes
Cluster Formation
Select PCH / Se-CH
Look Up Table
Select SCH
All CH
CH Checks if Avg. Distance >= Threshold between CH & CM
Set TX Power
Data Transfer
SCH will run H-AODV to find
CH will run H-AODV to find malicious nodes
Remove malicious nodes using alarm
On-line Mode

Figure 2 S^2-AODV in Offline Mode and On-Line Mode

3.1. M-AODV

Algorithm 1 shows how the protocol for Modified-AODV works, including the route discovery and maintenance processes. M-AODV overcomes the drawbacks of AODV by consuming less energy because it does not require a continuous broadcast for route change updates. Any node serving as a SN or an Intermediary Node (IN) in the network can use the algorithm. The source node begins sending and greeting the HELLO packets necessary to identify the nearby residents during the route discovery process. If the nodes are separated by 250 meters or less the two nodes are considered as neighbors. The Two new fields have been added to the HELLO packet format: willingness (0 to 7) and trust (0 to 1) according to our M-AODV algorithm. The threshold values of 0.5 and less than or equal to 3 are used for willingness and trust, respectively. Threshold values for willingness and trust are fixed firstly, based on the literature survey and also after running a few successful iterations satisfying the desired QoS parameter values.

```
N = {$N_1$, $N_2$, $N_3$, …………$N_n$} Set of N nodes in the network
For i = 1to N do
Discovery of neighbour nodes using
HELLO packets
Check for the [Willingness] and [Trust]
Update data received from neighbors
If
Willingness ≥ 3 and Trust ≥ 0.5
accept the neighbour and send RREQ
Else
Discard the neighbors
Search for new neighbours
End If
End For
```

Algorithm 1 Modified AODV (M-AODV)

3.2. H-AODV (Algorithm 3)

The algorithm primarily finds and eliminates numerous malevolent BH/GH attacks. Due to their ability to drop data packets between source and between SN and DN nodes, the two attacks are highly disruptive. In computer security, a honey-pot is a device that watches network traffic. They are a valid part of the network, just like the data and information that the attackers find to be of great worth. This is like putting out bait so the attackers become the victims and become the prey. M-AODV is used to partition the network into clusters, and then weight-based CH selection is applied. Algorithm 2 describes whether a node needs to join, exit, or declare itself as a gateway node (GW) if it is a part of two or more clusters (algorithm 3). Each CH will choose a random address (that doesn't exist in the network) as bait or destination addresses, broadcast the RREQ to all of its members, and inquire about the RREP from the members. Members that transmit RREP are the BH/GH nodes. The GW nodes and distributed GWs distribute this list throughout the entire network using the alert packet. The ALARM packet will contain a list of malicious nodes that need to be eliminated from the network. All nodes' routing tables will no longer contain the BH/GH nodes. Every T second, H-AODV will be carried out. In the event that the nodes do not respond, indicating that the network is secure, regular AODV will be used for route discovery, data transmission, and reception. The H-AODV process consists of two phases: the phase of detection and the phase of removal.

3.3. Detection Phase

During the detection stage, H-AODV is executed by every CH. The typical AODV is divided into two stages: route maintenance and route discovery. The CH node in H-AODV will send a route request with the destination address being a false honeypot address to catch malicious nodes and the source address being the address of the CH to each member of the cluster (as chosen by M-AODV). Each member of the cluster will look at the destination address but not reply because they do not have the route to that address. The BH and GH nodes will reply with an RREP to an RREQ sent by the CH node, indicating that they have the shortest path to the destination. The BH and GH nodes will reply with an RREP to an RREQ sent by the CH node, indicating that they have the shortest path to the destination. Black hole and grey hole nodes differ primarily in that the former will respond to all RREQs, while the latter will only do so under specific conditions. H-AODV uses the fact that malicious nodes react to all REEQ to trap them. Nodes, cluster heads, distributed gateway nodes, source nodes, destination nodes, and GW nodes make up each network.

3.4. Removal Phase (Algorithm 3, 4 & 5)

The CH nodes blacklist all such nodes as BH and GH nodes during the removal phase if they have responded to the CH nodes' RREQ with an RREP. The details of the identified BH/GH nodes are then communicated to the entire network via an ALARM packet sent by the CH nodes. This packet is then broadcast throughout the entire network by the distributed gateways (DGW) nodes, GW nodes, and CH nodes collaboratively. Every node using H AODV receives the blacklisted nodes via the ALARM packet. By simply deleting these malicious nodes from their routing table, all nodes eliminate the BH and GH nodes from the network as a whole.

```
For all nodes i
    o Each node broadcast HELLO
    o HELLO includes ID, ID_MEMBER, SPEED, WEIGHT
      and STATE
    o Each node initially is in UNCLUSTERED state
```

```
o All HELLO is added to the routing table WEIGHT comparison
o Node with highest WEIGHT announces itself as the ID_CH
End For
```

Algorithm 2 CH Selection

```
For all nodes i
o Only if LLT ≥ Threshold between node and CH Node can join a cluster
o If (a node receives HELLO from 2 or more CHs (Overlapped Zone))
o && (both LLT values are ≥ Threshold it will join both the clusters) Call itself gateway node
o Elseif (only one of the LLT is ≥ Threshold it will join that cluster)
o && (none of the LLT is ≥ Threshold it will be called an ORPHAN node) and will be in UNCLUSTERED state
o End If
o If (2 nodes from different clusters can hear each other (Non-Overlapped Zone))
o These 2 nodes will declare themselves as the Scattered GW nodes
o Broadcast this message within their clusters
o End if
End For
```

Algorithm 3 Cluster Join Algorithm

```
o Works in II phases: Cluster re-election and member handover
o If (2 CHs meet; who has the larger weight will be the new CH)
o The new CH will broadcast its ID
o Members who can meet the required LLT will join the new CH
o Other members will again go to ORPHAN state
End If
```

Algorithm 4 Cluster Maintenance

```
o For all CHs
o After every T seconds run H-AODV with DEST address as bait address
o If (Reply from the other nodes)
o List all the nodes with RREPs as the malicious nodes
o Make the BH node list
o Send alarm packets to the entire network through GW nodes, Scattered GW nodes and Sink node
o All the nodes in the network will remove the listed nodes from their routing table
o Else
o Regular AODV protocol to find the route from source to destination
o Data transmission and reception
o End If
End For
```

Algorithm 5 Co-Operative Blackhole Detection (H-AODV)

3.5. Proposed S^2-AODV in Off-Line Mode

Once the network is established, the clusters are formed using HELLO packets and M_AODV in algorithm 1. The primary and secondary CH are formed using the weight-based CH selection. Based on the weight the primary and secondary CH nodes are selected. Also, the weight values from all CH nodes are compared to select the SCH node.

CH nodes collect the information like RSSI (1)(2)(3), Transmission power (TXP) (0-10dBm), speed from each of its members. This data is collected for different distances, with different TXP and different mobility. This data is fed to the ML algorithms like random forest, Naïve Bayes, Decision tree and SVM algorithms. From the data set the link quality between the CH and CM nodes are divided into three categories good, bad, and medium. This categorization is based on distance between CH and CM nodes. Random forest algorithm gave the highest efficiency in determining the link quality between CH and CM. After running for multiple iterations, the conclusion is as shown in Table 2. The iterations were carried out with fixed TXP power of the CH nodes with varying node speeds and varying distances. Based on the average distance between the CH and CM, the algorithm clearly divides the data set into three classes as shown in table 2. This look up table is shared by the SCH node to each CH after every 't' seconds. Based on this the CH nodes will either increase or decrease their TXP. This enhances the energy efficiency in the network. Table 3. shows the simulation parameters using NS-2.34.

The following are the calculations. Notations used in the calculations are shown in Table (1)

RSSI calculation (Two-ray ground propagation model):

$$P_r(d) = \frac{Pt * G^2 * {H_t}^2 * {H_r}^2}{d^4 * \mathrm{L}} \qquad (1)$$

RSSI calculation (Free space propagation model):

$$P_r(d) = \frac{Pt * G * \lambda^2}{(4\pi^2) * d^2 * L} \qquad (2)$$

RSSI calculation (Free space propagation model):

$$\frac{Pr(R)}{Pr(A)} = \left[\frac{A}{R}\right]^{\beta} \qquad (3)$$

Table 1 Details of Notations Used in Equation (1 to 3)

Pr(d)	Power Received from a Distance
Pt	TX Power
G	Transmitter gain * Receiver gain
H_t	antenna height (Transmitting)
H_r	height (receiving antenna)
D	Distance from the transmitter
L	Path Loss
A	Actual distance
R	Reference distance
Β	Path loss exponent

Table 2 Look up Table for CH Nodes

Sl. No	Range (meters)	Power (dBm)
1	0 – 110	0 dBm
2	110 - 220	Decrease by 1 dBm
3	220 - 250	Increase by 1 dBm

3.6. S^2-AODV in On-Line Mode for Security Enhancement

As seen in the previous discussion offline mode is purely for clustering and enhancing the battery efficiency and hence network lifetime is enhanced. The CH nodes are trained to efficiently use the transmitting power based on the distance and RSSI collected from the Cluster Members (CM). Based on these parameters various Machine Learning (ML) algorithms such as Naive Bayes, Random Forest, Decision Tree, and SVM are used to analyze the link quality between the CH node and CMs. Based on this analysis the link quality between CH and CM are categorized into 3 different classes namely good, medium, and bad. According to the results, the random forest algorithm performs better in terms of data classification efficiency. Several iterations with varying networking parameters like varying node Transmission Power (TXP), distance, mobility is carried out. According to the classification from ML algorithms a look-up table is created (Table 2) indicating the TXP to be set by the CH nodes. SCH can distribute the look-up table to CH nodes in order to set their TXP and improve network battery efficiency and enhance the lifetime. In on-line mode, SCH executes H-AODV to identify and eliminate the network's malevolent CH (black hole/gray hole) nodes. Hence the name smart as the nodes uses the battery very smartly and securely because of H-AODV run by SCH n odes and CH nodes. There are several algorithms available to detect and avoid malicious nodes. But they are suitable for single attack removal or in static environments like WSNs. Existing papers assume that the SN, DN and the CH node are always legitimate nodes. Our work is an enhancement over such approach where we don't assume anyone to be legitimate. The SCH node will send look up table (Table 2) to all the CH nodes to set their TXP to the values according to the range specified. The range is the average distance between CH and all the CM nodes. According to the look up table each CH will set their TXP. The SCH node uses the ALARM packets to identify and eliminate the malicious CH nodes from the network using the H-AODV algorithm. H-AODV is another program that CH nodes use to identify and eliminate malicious nodes from their network. As shown below (algorithm 6).

- For all nodes 'i'
- Find neighbors using M-AODV
- Perform Primary / Secondary selection using CH selection
- Perform weight-based SCH selection
- Among all CH highest weight will be SCH
- Cluster join algorithm
- Cluster maintenance algorithm
- SCH node will circulate the look up table to all CH nodes
- CH nodes will perform Co-operative Blackhole detection (H-AODV)
- SCH nodes perform Co-operative Blackhole detection (H-AODV)
- Detect and remove the malicious nodes using ALARM packets
- Calculate the various network QoS parameters
- Compare AODV, M-AODV, H-AODV, C-SSA with S^2-AODV
- End

Algorithm 6 Smart Secure (S^2-AODV) Online Mode

4. RESULTS AND DISCUSSION

The work is an enhancement on the AODV protocol, with the energy efficiency and security features added. All results are depicted with 100 nodes with each cluster having 10 cluster members. 5 to 20 % of them being malicious nodes with the random way point mobility model and two-ray ground propagation model. Scalability of the network is checked. S^2-AODV works very efficiently compared to AODV and C-SSA in all cases. Different malicious node percentages were tried based on the number of nodes in the network. In each case S^2-AODV outperforms the AODV, M-AODV, H-AODV and C-SSA for the parameters like throughput, PDR, latency, detection rate. The influence of the mobility models and propagation models on different algorithms are also depicted in the results.

The free-space model depicted in Figure 3 is the most basic model. Perfect line-of-sight propagation and a single path connecting the transmitter and receiver are prerequisites for it. The two-ray ground reflection model, as depicted in Figure 4, takes into account both the direct path and a ground reflection path. As in the free space model, line of sight is required for both the transmitter and the receiver nodes. It has been shown that this model outperforms the free space model in the case of a long line of sight path. Both the Free space model and the Two-ray model predict the received power [33] as a deterministic function of the transmitter and receiver distance. There is greater accuracy in the shadowing model. It contributes to the deterministic path loss (e.g., fading) and increases the random component of received power, which aims to replicate the random variability common in wireless networks. The two parts of the shadowing model are the deterministic path loss, which estimates the received power depending on the separation between the transmitter and receiver nodes, and the variation of the received power at particular distances. It is an undeniable fact that models of propagation and mobility impact a network's performance. Models of random mobility such as Random Walk, Random Direction, and Random Way Point are more akin to real-world situations. Propagation models equally affect the network performance of any mobile network. Most used propagation models are free space, two-ray ground, shadowing model. Hence all above mentioned models are considered to evaluate the performance of the proposed work. Performance evaluation and comparison with the existing techniques are also done.

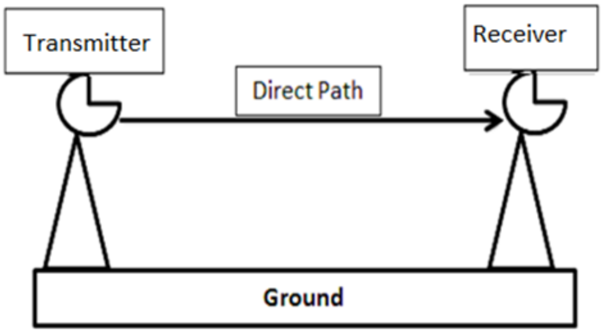

Figure 3 Model of Free Space

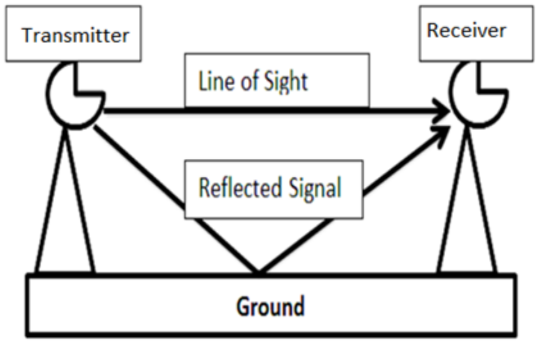

Figure 4 Two Ray Ground Model

Calculation of parameters:

Average Throughput =

$$\sum_{i=1}^{n} \frac{Total\ received\ packets\ i*packet\ size}{Total\ simulation\ time} \quad (4)$$

Average Delay =

$$\sum_{i=1}^{n} \frac{Received\ time\ \ i-\ Sent\ time\ i}{Total\ data} \quad (5)$$

Average Detection rate =

$$\sum_{i=1}^{n} \frac{detection\ time\ \ i-\ inserted\ time\ \ i}{Total\ simulation\ time} \quad (6)$$

Average energy consumption =

$$\sum_{i=1}^{n} \frac{initial\ energy - available\ enrgy\ at\ \ time\ i}{Total\ simulation\ time} \quad (7)$$

Table 3 Simulation Parameters

Parameter	**Values**
Simulation time	200s
Simulation area	3000m by 3000m
Number of nodes	50, 100, 150
TXP	15dBm
Node speed (random)	Arbitrary (0–25 m/s)
Packet size	512 bytes
Traffic type	CBR(UDP)
Mobility model	Random Walk, Random Direction, and Random Way Point
Propagation model	Free space, two-ray ground, shadowing model
Radio range	250m
Initial TRP for each node	10 dBm

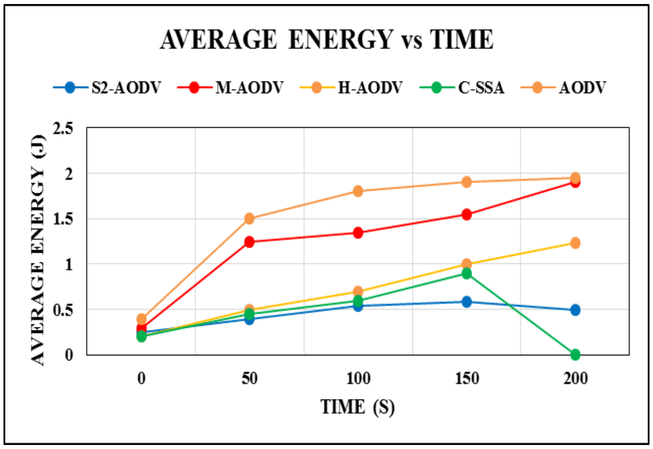

Figure 5 Average Energy Consumption Vs Time

Figure 5 displays the average energy consumption of the network in relation to simulation time using a two-ray ground propagation model, a random-way point mobility model, and 100 nodes. Average energy consumption of the network is calculated using equation (7) as shown above. It is very clearly seen that the proposed algorithm S^2-AODV outperforms AODV, M-AODV, H-AODV and C-SSA. Energy consumption is affected due to mobility of the nodes, available TXP with CH nodes and due to resource wastage by the malicious nodes. All the issues are addressed in the proposed model and to a certain extent by the C-SSA algorithm. AODV has no such technique to save energy hence it performs the least. In M-AODV neighbor selection is based on remaining energy so the performance is better, but it does not have malicious node detection process. H-AODV uses baiting for malicious node detection but has no energy efficiency enhancement.

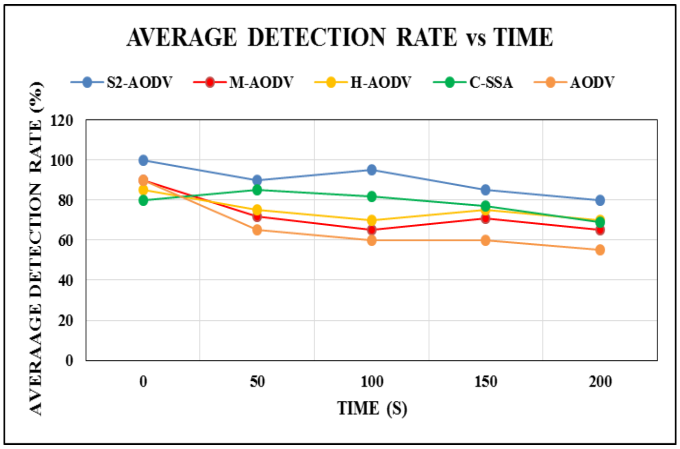

Figure 6 Average Detection Rate Vs Time

Average Detection rate is calculated based on equation (6). Results in Figure 6 demonstrate the detection rate and detection delay of S^2-AODV and C-SSA are better than H-AODV, M-AODV and AODV. The proposed algorithm does not assume any node to be a legitimate node and can detect malicious CH nodes. The algorithm detects faster as the network energy efficiency is also taken care of. C-SSA assumes the source node, destination node and CH nodes to be legitimate. C-SSA does not specify the number of malicious nodes in the network. Hence performance-wise C-SSA is almost the same as the proposed algorithm. But all other protocols are showing poor performance as they do not address malicious node detection, or they poorly address the issue.

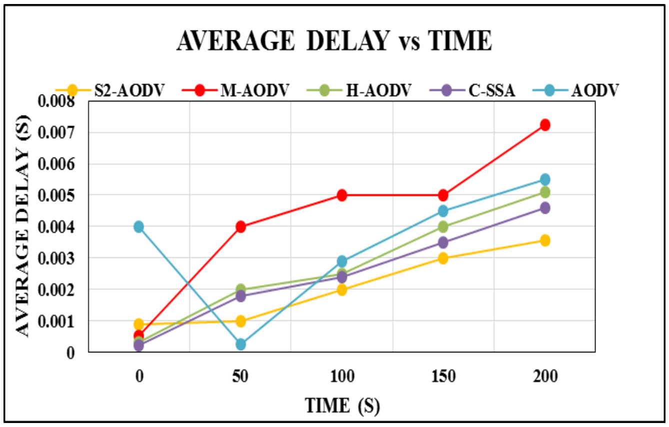

Figure 7 Average Delay Vs Time

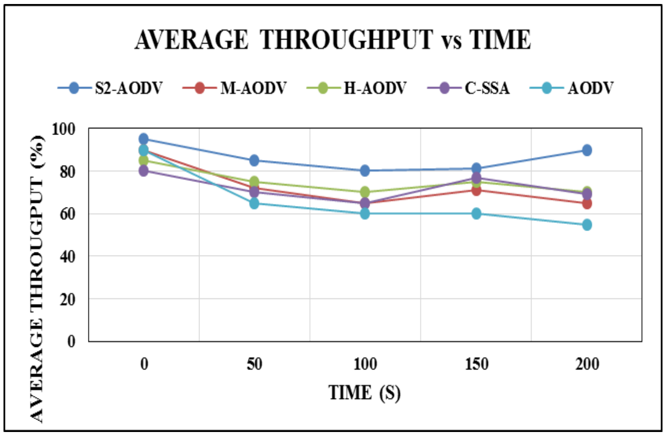

Figure 8 Average Throughput Vs Time

Average delay is calculated using equation (5). Figure 7 shows the Average delay v/s time. Average delay is the delay in communicating packets to the destination node due to this detection process. The delay for the proposed algorithm is very less. That means there is not much overhead caused due to the entire process in S^2-AODV compared to C-SSA, H-AODV, M-AODV and AODV. The overhead is less as the new node SCH along with CH nodes will take care of the malicious activity in the network. This in turn enhances the throughput and PDR of the network.

Average network throughput shown in equation (4) is the total number of packets delivered over a given period of time in the network. Throughput of S^2-AODV compared to C-SSA, H-AODV, M-AODV and AODV is better as shown in Figure 8. Between 50s to 100s there is a slight dip in the performance, as during that time the malicious nodes may have entered the network. But due to H-AODV executed by SCH node and CH nodes the throughput is again improved. In C-SSA there are direct trust, indirect trust, and recent trust which each CH node must calculate. Also, there is a fitness function which tells whether the node is fit to be in the cluster. This will cause delays; overheads will be increased, and throughput is reduced.

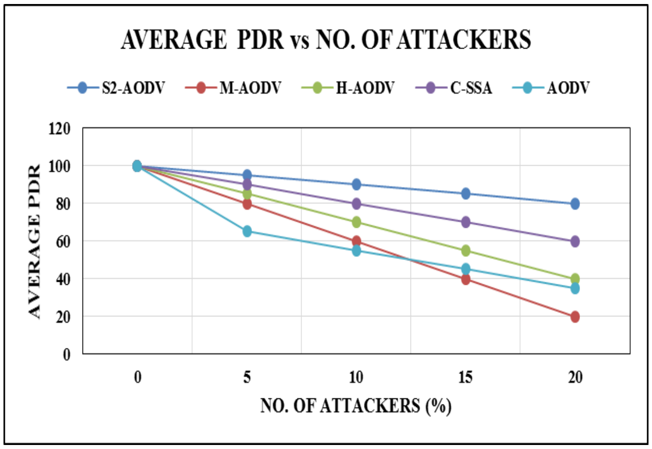

Figure 9 Average PDR Vs No. of Attackers

PDR is defined as the ratio of all packets sent and received over a given network. In this case also PDR of S^2-AODV compared to C-SSA, H-AODV, M-AODV and AODV is better as shown in Figure 9. The reason being the use of various ML algorithms used to generate the look-up table. This table is circulated to all the CH nodes by the SCH node at regular time intervals. This enhances energy efficiency and the PDR of the network. Same is not the case in all other algorithms.

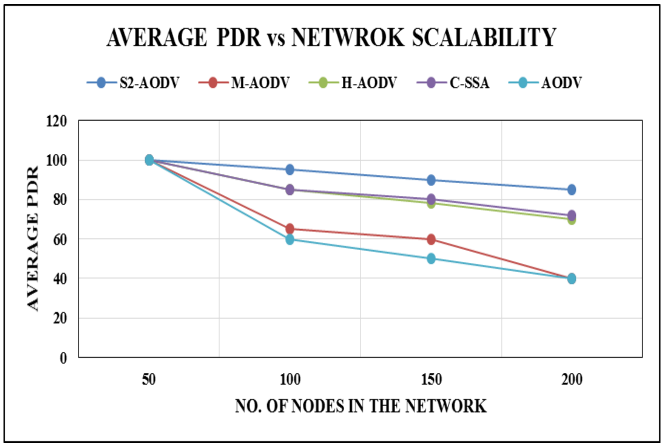

Figure 10 Average PDR Vs Network Scalability

Scalability is a major due to the mobility of the nodes in MANETs, a worry with no fixed topology. Security issues are also of major concern as there is no centralized control in the network. One attacker can launch multiple attacks. The proposed algorithm S^2-AODV addresses the scalability issue (Figure 10) as the network energy and security are taken care of and the algorithm works good for small, medium, and large size networks also. In C-SSA only node battery is measured as a part of fitness function and the work does not address the TXP issues. H-AODV, M-AODV and AODV assume certain nodes are always good nodes which may not be true in most of the cases. This affects the PDR and network scalability.

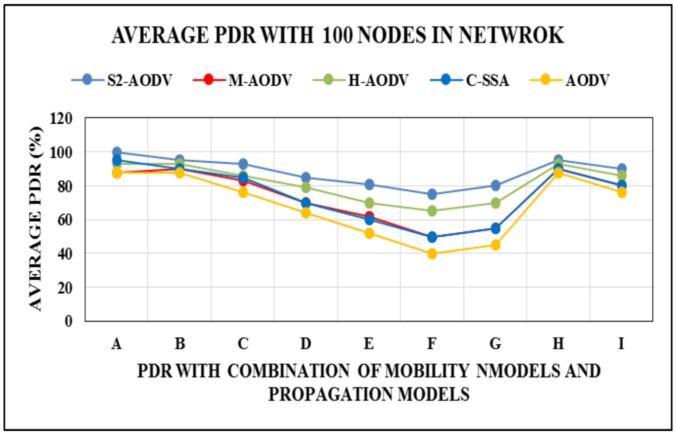

Figure 11 Average PDR with 100 Nodes in Network

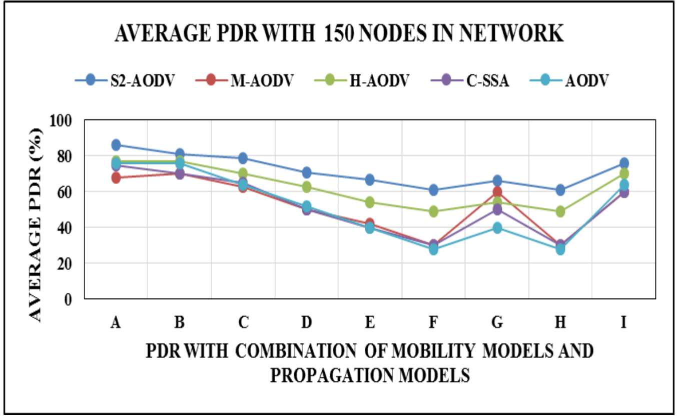

Figure 12 Average PDR with 150 Nodes in Network

The performance of any MANETs is greatly influenced by the mobility models and propagation models. Various combinations of propagation and mobility models carried out are shown in Table 4. For different combinations of random mobility models and propagation models, PDR with 150 and 100 nodes respectively in the network is calculated. S^2-AODV compared to C-SSA, H-AODV, M-AODV and AODV is better. The performance for certain combinations is better than other combinations. From the graphs in Figure 11 and 12 it is evident that the combination of random way point with the best results are obtained with the two-ray ground model and the random direction with free space model.

Table 4 Details of X-Axis Values of Figure 11 and Figure 12

A	Random way point with two-ray ground model	D	Random walk with two-ray ground model	G	Random direction with two-ray ground model
B	Random way point with free space model	E	Random walk with free space model	H	Random direction with free space model
C	Random way point with shadowing model	F	Random walk with shadowing model	I	Random direction with shadowing model

5. CONCLUSION AND FUTURE SCOPE

Security and power optimization approaches are addressed in the paper. The S^2-AODV is an enhancement over reactive AODV with M-AODV and H-AODV integrated in it along with an extra power optimization feature. Power optimization was done efficiently with random forest algorithm. The network is divided into clusters using M-AODV algorithm. M-AODV is modified AODV with 2 parameters added like willingness and trust between the nodes. A node will be considered as a neighbor only if the willingness is above 3 and trust is above 0.5. As a part of H-AODV algorithm weight of the neighboring nodes is considered for the CH selection. Weight of the node is dependent on the stability, constancy, and largest neighbor factor. Each CH node runs a baiting algorithm with a random destination address which does not exist in the network. Nodes which reply to such packets are malicious nodes (BH/GH). S^2-AODV works in off-line mode and on-line mode. In offline mode, each CH collects the RSSI, TXP and node mobility. The dataset is generated with different scenarios like varying speeds of the nodes, with varying TXP power levels and varying distances. Same is fed to SVM, random forest, Naïve Bayes' and decision tree. Random forest gave the efficiency of 92% with the distance-based bifurcation. After many iterations a look-up table was generated. This table is fed as input by SCH node to all the CH nodes which set their TXP based on this table. SCH node also runs H-AODV to find malicious CH nodes. CH nodes will run H-AODV to remove malicious nodes in their network. Algorithm supports the various models of mobility and propagation models. It was discovered that the random way point mobility model combined with the free space propagation model produced better results. Finally, the performance of the S^2-AODV is found to be better in terms of delay, detection rate, throughput, detection delay and scalability as compared with AODV, M-AODV, H-AODV and C-SSA. As a future scope more cross layer parameters can be added to eliminate the BH/GH nodes from the network. The algorithm can be checked for other active attacks in the network like Sybil and wormhole attacks.

REFERENCES

[1] S. Uppalapati, ‘‘Energy-efficient heterogeneous optimization routing protocol for wireless sensor network,’’ Instrum. Mesure Metrol., vol. 19, no. 5, pp. 391–397, Nov. 2020.

[2] S. Bharany, S. Sharma, S. Badotra, O. I. Khalaf, Y. Alotaibi, S. Alghamdi, and F. Alassery, ‘‘Energy-efficient clustering scheme for flying Ad-Hoc networks using an optimized LEACH protocol,’’ Energies, vol. 14, no. 19, p. 6016, Sep. 2021.

[3] U. Srilakshmi, N. Veeraiah, Y. Alotaibi, S. A. Alghamdi, O. I. Khalaf, and B. V. Subbayamma, ‘‘An improved hybrid secure multipath routing protocol for MANET,’’ IEEE Access, vol. 9, pp. 163043–163053, 2021.

[4] B. Rajkumar and G. Narsimha, ‘‘Secure multipath routing and data transmission in MANET,’’ Int. J. Netw. Virtual Organisations, vol. 16, no. 3, pp. 236–252, 2016.

[5] G. Anjaneyulu, V. M. Viswanatham, and B. Venkateswarlu, ‘‘Secured and authenticated transmission of data using multipath routing in mobile AD-HOC networks,’’ Adv. Appl. Sci. Res., vol. 2, no. 4, pp. 177–186, 2011.

[6] R. Prasad P and S. Shankar, ‘‘Efficient performance analysis of energy aware on demand routing protocol in mobile Ad Hoc network,’’ Eng. Rep., vol. 2, no. 3, p. e12116, Mar. 2020.

[7] S. V. Kumar and V. AnurathaEnergy, ‘‘Efficient routing for MANET using optimized hierarchical routing algorithm (Ee-Ohra),’’ Int. J. Sci. Technol. Res., vol. 9, no. 2, pp. 2157–2162, Feb. 2020.

[8] N.-C. Wang and Y.-L. Su, ‘‘A power-aware multicast routing protocol for mobile Ad Hoc networks with mobility prediction,’’ presented at the IEEE Conf. Local Comput. Netw. 30th Anniversary (LCN)l, Sydney, NSW, Australia, Nov. 17, 2005, p. 8 and 417.

[9] R. Rout, P. Parida, Y. Alotaibi, S. Alghamdi, and O. I. Khalaf, ‘‘Skin lesion extraction using multiscale morphological local variance reconstruction-based watershed transform and fast fuzzy C-Means clustering,’’ Symmetry, vol. 13, no. 11, p. 2085, Nov. 2021.

[10] U. Venkanna, J. K. Agarwal, and R. L. Velusamy, ‘‘A cooperative routing for MANET based on distributed trust and energy management,’’ Wireless Pers. Commun., vol. 81, no. 3, pp. 961–979, Apr. 2015.

[11] M. Bharti, S. Rani and P. Singh, "Security Attacks in MANET: A Complete Analysis," 2022 6th International Conference on Devices, Circuits and Systems (ICDCS), 2022, pp. 384-387, doi: 10.1109/ICDCS54290.2022.9780760.

[12] M. Bharti, S. Rani and P. Singh, "Security Attacks in MANET: A Complete Analysis," 2022 6th International Conference on Devices, Circuits and Systems (ICDCS), Coimbatore, India, 2022, pp. 384-387, doi: 10.1109/ICDCS54290.2022.9780760..

[13] R. I. Al-Essa and G. A. Al-Suhail, "Mobility and Transmission Power of AODV Routing Protocol in MANET," 2022 2nd International Conference on Computing and Machine Intelligence (ICMI), 2022, pp. 1-5, doi: 10.1109/ICMI55296.2022.9873686.

[14] M. D. Chawhan, K. Karmarkar, G. Almelkar, D. Borkar, K. D. Kulat and B. Neole, "Identification and prevention of Gray hole attack using IDS mechanism in MANET," 2022 10th International Conference on Emerging Trends in Engineering and Technology - Signal and Information Processing (ICETET-SIP-22), 2022, pp. 1-6, doi: 10.1109/ICETET-SIP-2254415.2022.9791594.

[15] M. M. Hamdi et al., "A study review on Gray and Black Hole in Mobile Ad Hoc Networks (MANETs)," 2022 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), 2022, pp. 1-6, doi: 10.1109/HORA55278.2022.9800011.

[16] M. P. Kumar, M. M. Kumar, S. Shobana, L. Padmanaban, A. Nageswaran and R. Krishnamoorthy, "Enhanced Secure Routing in

MANET using Collaborative Machine Learning Approach," 2022 8th International Conference on Smart Structures and Systems (ICSSS), 2022, pp. 1-6, doi: 10.1109/ICSSS54381.2022.9782205.

[17] D. N. M. Hoang, J. M. Rhee and S. Y. Park, "Fault-Tolerant Ad Hoc On-Demand Routing Protocol for Mobile Ad Hoc Networks," in IEEE Access, vol. 10, pp. 111337-111350, 2022, doi: 10.1109/ACCESS.2022.3216066.

[18] P. Upadhyay, V. Marriboina, S. Kumar, S. Kumar and M. A. Shah, "An Enhanced Hybrid Glowworm Swarm Optimization Algorithm for Traffic-Aware Vehicular Networks," in IEEE Access, vol. 10, pp. 110136-110148, 2022, doi: 10.1109/ACCESS.2022.3211653.

[19] U. Srilakshmi, S. A. Alghamdi, V. A. Vuyyuru, N. Veeraiah and Y. Alotaibi, "A Secure Optimization Routing Algorithm for Mobile Ad Hoc Networks," in IEEE Access, vol. 10, pp. 14260-14269, 2022, doi: 10.1109/ACCESS.2022.3144679.

[20] X. Chen, G. Sun, T. Wu, L. Liu, H. Yu and M. Guizani, "RANCE: A Randomly Centralized and On-Demand Clustering Protocol for Mobile Ad Hoc Networks," in IEEE Internet of Things Journal, vol. 9, no. 23, pp. 23639-23658, 1 Dec.1, 2022, doi: 10.1109/JIOT.2022.3188679.

[21] M. Sharma, P. Kumar and R. S. Tomar, "Weight-Based Clustering Algorithm for Military Vehicles Communication in VANET," in SAIEE Africa Research Journal, vol. 114, no. 1, pp. 25-34, March 2023, doi: 10.23919/SAIEE.2023.9962790.

[22] M. M. Gaber and M. A. Azer, "Blackhole Attack effect on MANETs' Performance," 2022 2nd International Mobile, Intelligent, and Ubiquitous Computing Conference (MIUCC), 2022, pp. 397-401, doi: 10.1109/MIUCC55081.2022.9781680.

[23] N. Veeraiah, O. I. Khalaf, C. V. Prasad, Y. Alotaibi, A. Alsufyani, S. A. Alghamdi, and N. Alsufyani, ''Trust aware secure energy efficient hybrid protocol for MANET,'' IEEE Access, vol. 9, pp. 120996–121005, 2021.

[24] A. Mallikarjuna and V. C. Patil, ''PUSR: Position update secure routing protocol for MANET,'' Int. J. Intell. Eng. Syst., vol. 14, no. 1, pp. 93–102, Feb. 2021.

[25] M. Rajashanthi and K. Valarmathi, ''A secure trusted multipath routing and optimal fuzzy logic for enhancing QoS in MANETs,'' Wireless Pers. Commun., vol. 112, no. 1, pp. 75–90, May 2020.

[26] R. Nithya, K. Amudha, A. S. Musthafa, D. K. Sharma, E. H. Ramirez-Asis, P. Velayutham, V. Subramaniyaswamy, and S. Sengan, ''An optimized fuzzy based ant colony algorithm for 5G-MANET,'' CMC-Comput., Mater. Continua, vol. 70, no. 1, pp. 1069–1087, 2022

[27] S. R. Halhalli, S. R. Sugave, and B. N. Jagdale, ''Optimisation driven-based secure routing in MANET using atom whale optimisation algorithm,'' Int. J. Commun. Netw. Distrib. Syst., vol. 27, no. 1, p. 77, 2021.

[28] V. Alappatt and J. P. P. M., ''Trust-based energy efficient secure multipath routing in MANET using LF-SSO and SH2E,'' Int. J. Comput. Netw. Appl., vol. 8, no. 4, p. 400, Aug. 2021.

[29] K. K. Thangadorai et al., "Intelligent and Adaptive Machine Learning-based Algorithm for Power Saving in Mobile Hotspot," 2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC), 2020, pp. 1-6, doi: 10.1109/CCNC46108.2020.9045535.

[30] Jie Gu, Shan Lu,An effective intrusion detection approach using SVM with naïve Bayes feature embedding, Computers & Security,Volume 103,2021,102158,ISSN 0167-4048, https://doi.org/10.1016/j.cose.2020.102158.

[31] J. Ryu and S. Kim, "Reputation-Based Opportunistic Routing Protocol Using Q-Learning for MANET Attacked by Malicious Nodes," in IEEE Access, doi: 10.1109/ACCESS.2023.3242608.

[32] N. Veeraiah and B. T. Krishna, ''An approach for optimal-secure multi-path routing and intrusion detection in MANET,'' Evol. Intell., vol. 5, pp. 1–15, Mar. 2020.

[33] S. Palanisamy, B. Thangaraju, O. I. Khalaf, Y. Alotaibi, S. Alghamdi, and F. Alassery, ''A novel approach of design and analysis of a hexagonal fractal antenna array (HFAA) for next-generation wireless communication,'' Energies, vol. 14, no. 19, p. 6204, Sep. 2021.

[34] Sampada H K, Dr. Shobha K R.: Performance Analysis of Energy Efficient MANETs- using MODIFIED AODV (M-AODV). In: © Springer Nature Singapore Pte Ltd. 2019.S. Lecture Notes on Data Engineering and Communications Technologies 15, https://doi.org/10.1007/978-981-10-8681-6_9.

[35] Sampada H K, Shobha K R., "Cluster-Based – Multiple Malicious Node Detection using Honeypot AODV (H-AODV) in MANETs", Int. J. of Communication Networks and Distributed Systems, 30 (1), PP:1-29, 2023.

[36] S. K. Prasad, S. Gupta, R. B. Singh and T. Sharma, "Performance Testing of AODV using Channel Fading for MANETs," 2022 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COM-IT-CON), 2022, pp. 811-816, doi: 10.1109/COM-IT-CON54601.2022.9850951.

[37] A. Jain, U. Prajapati and P. Chouhan, "Trust based mechanism with AODV protocol for prevention of black-hole attack in MANET scenario," 2016 Symposium on Colossal Data Analysis and Networking (CDAN), 2016, pp. 1-4, doi: 10.1109/CDAN.2016.7570866.

[38] Naseeruddin and V. C. Patil, "Performance evaluation of MANET protocols: A propagation model perspective," 2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), 2016, pp. 55-61, doi: 10.1109/ICATCCT.2016.7911965.

[39] Altaf Hussain, "ERWPM-MANET: Evaluation of Radio Wave Propagation Models in Mobile Ad Hoc Network by using Distance Scenario", Romanian Journal of Information Technology and Automatic Control, Vol. 32, No. 2, 35-50, 2022.

[40] P. Ghosh and D. Verma, "An Improved Reputation Based Approach for Malicious Node Detection System in Manet," 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), 2022, pp. 275-277, doi: 10.1109/ICACITE53722.2022.9823753.

Authors

Dr. Sampada H K completed her M.-Tech. in Digital Communication and Networking in the year 2004 from SJC Institute of Technology (SJCIT), Chikballapur, under Visvesvaraya Technological University (VTU). She has completed her Ph.D. under VTU, in the department of TCE, MSRIT, Bengaluru. She is currently working as Assistant Professor in the department of ECE, Atria IT, Bengaluru. Her research interests are in security issues in Mobile Ad Hoc Networks, VANETs, IoT and Data Science. She has presented her research papers in several international conferences and Journals.

Dr. Shobha K R received her M.E. degree in Digital Communication Engg from Bengaluru University, Karnataka, India and Ph.D. from Visveswaraya Technological University. She is currently working as an Associate Professor in the department of Electronics & Telecommunication Engineering, M.S. Ramaiah Institute of Technology, Bengaluru. Her research areas include Mobile Ad Hoc Networks, IoT and Cloud Computing. She has more than 25 Papers publications to her credit. She is a Senior IEEE Member serving as Secretary of IEEE Sensor Council, Bengaluru Section. She is also an active member of IEEE Communication Society and Women in Engineering under IEEE Bengaluru Section.

RESEARCH ARTICLE

How to cite this article:

Sampada H K, Shobha K R, "Co-Ordinated Blackhole and Grayhole Attack Detection Using Smart & Secure Ad Hoc On-Demand Distance Vector Routing Protocol in MANETs", International Journal of Computer Networks and Applications (IJCNA), 11(1), PP: 13-28, 2024, DOI: 10.22247/ijcna/2024/224433.