An Optimized and Hybrid Energy Aware Routing Model for Effective Detection Of Flooding Attacks in a Manet Environment

Mallikarjuna Nandi (mallikarjuna.nandi2019@vitstudent.ac.in)
VIT University - Chennai Campus
Anusha Kannan
VIT University - Chennai Campus https://orcid.org/0000-0002-8391-1744

Research Article

Keywords: Malicious nodes, ANFIS classifier,Flooding attacks, AODV, Security Mobile Agent (SMA), Ant Colony Optimization (ACO), Fitness Distance Ratio Particle Swarm Optimization (FDR PSO)

Posted Date: June 15th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-586844/v1

AN OPTIMIZED AND HYBRID ENERGY AWARE ROUTING MODEL FOR EFFECTIVE DETECTION OF FLOODING ATTACKS IN A MANET ENVIRONMENT

[1]*Mallikarjuna Nandi*
Research Scholar, SCOPE,
Vellore Institute of Technology, Chennai, India.
E-mail: mallikarjuna.nandi2019@vitstudent.ac.in

[2]K.Anusha
Associate Professor, *SCOPE,*
Vellore Institute of Technology, Chennai, India.
E-mail: anusha.k@vit.ac.in

Abstract: *Ad Hoc networks for communication have completely replaced the existing communication technologies which are dependant on infrastructure. An attractive and widely utilized field in communication systems is Mobile Ad Hoc Networks or the MANETs which are a derivative of the conventional Ad Hoc Networks. Security of information communicated through MANETs as well as the robust nature of the network is a prime issue of concern and research in recent times. Amongst various attacks prevalent on MANET environment, packet flooding is a common attack and causes a devastating effect on MANET nodes which if left undetected may lead to consequent crashing of the entire network. Floodding attacks also tend to consume enormous energy well above the prescribed energy consumption limits per node resulting in lifetime reduction. Hence, detection of these malicious nodes and their differentiation from trustworthy nodes is taken as the research objective in this paper. This paper presents feature extraction anda classification model based on ANFIS (Adaptive Neuro-Fuzzy Inference System). By using ANFIS classifier, the extracted featureis trained and then classified.Further to counter the flooding cum energy preserving routing, this paper proposes a SMA integration with AODVprotocol called SMA$_2$AODV to detect flooding attacks for MANETs. After detecting, the hybrid model ACO combined with FDR PSO for optimizing energy. ACO-FDR PSO identifies the energy-efficient routeand minimizes energy consumption in the network, toincrease node lifetime that ensures energy-efficient routing. The performance metrics like throughput, packet delivery ratio, attack detection ratio, and energy consumption areanalyzedby using the NS-2 simulator with existing benchmark methods.*

KeywordsMalicious nodes, ANFIS classifier,Flooding attacks, AODV, Security Mobile Agent (SMA), Ant Colony Optimization (ACO), Fitness Distance Ratio Particle Swarm Optimization (FDR PSO)

1.INTRODUCTION

A MANET is used for affording communication processes by using a wireless link that does not rely on any topology network. It contains wireless nodes that forma temporary network that does not have the infrastructure and here the nodes will communicate by multi hops. The MANET nature is self-organized and distributed for performing the functionality of the desired network by node participation and node cooperation which is vital to provide effective communication. The challenges in MANET are routing, security, access control, reliability, and energy consumption. These challenges are addressed by deploying a routing protocol securely and that can find the malicious nodes and separate them from the communication network for increasing performance.Security is important in data communication in MANETs. Security attacks are mainly through packet flooding on the network consuming more energy and thereby creating a congestion which gets converted into a Denial of Service (DoS) attack. A trusted routing helps for avoiding communicating risk by untrusted nodes.Trust management is necessary for MANETs to increase security in less infrastructure communication mode [1]..In AODV, routing protocols are mainly used for routing that works by on-demand model for identifying routes. Security variables are added in the route reply and discovery by varying packet respectively. Another design problem for an efficient protocol design is mobility speed and energy consumption. For network design, the nodes are employed initially followed by a decrease in their mobility.They are then allowed for only moving when needed under mandatory circumstances. More mobility in a system of MANET causes decreased throughput and which increases packet drop ratio. The existence of nodes in process routing creates flooding attacks which will consume more energy. It is decreased by presenting a routing protocol based on a clustering method in which the size of a cluster will be dynamically decided depending on the degree and distance of node mobility. It is needed for enhancing the AODV protocol by extra features such ascluster-based routing,security, agent-based communication, and then awareness of energy routing.Cluster formation is an activity for designing a clustering network. It enhances the overhead control in high-density scenario nodes. Also, cluster numbers are optimally formed by taking total node numbers, node distance, and node mobility.Awide network is split into smaller numeral networks by implementing process clustering. For every cluster,CH is periodically elected by assigning a node called cluster head reliably and for performing effective communication by using CH. Every node inside a cluster should communicate through CH for sending and receiving of packets. And then, a node in a cluster will

communicate to the other cluster node by their cluster heads respectively. The node that is nearer to CHs needs low energy for their communication and while distant nodes will spend high energy for their communication [2]. Moreover, if every packetis routed by the node that is nearer to CH, that node can lose its energy more fast. For dividing routing packets load, every node is allowed to taking parts in process of routing. Itwill be reached through minimal spanning tree forming that contains cluster nodes and for performing the routing by the shortest route.The CEESRA is also used to provide efficient routing that is done in MANET. The routing design is made capable of adapting itself to novel environments when there is frequently varying in topology network. More existing designs i.e. routing in Ad Hoc networks are implemented by considering distance metrics and static nodes. However, for choosing CH,only distances are not metric, but also energy is considered to provide asafe routing design. Additionally in clustering, the length path for CH istaken as an important metric for maximizing lifetime network byoptimal energy. The important benefit for this optimized energy by using a process of clustering is easily avoided and identified malicious nodes.Therefore, the present efficient energy secure routing design will consider nodes hop distance, CH hop distance, the energy needed to make decisions for routing.However, cluster models are used in the layer of routing depend on hops number and also uses a minimal spanning tree. The advantage is providing secured and reliable data transmission by agents to perform cluster, routing, and energy management.

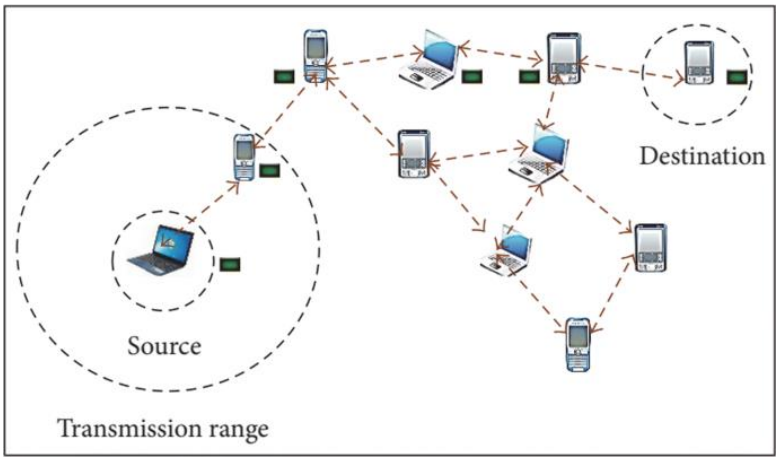

Fig. 1 MANET architecture scenario

MANET is a heterogeneous node that will communicate without a facility like routers or base stations. InMANETs, communication between mobile nodesis done by using transmissions like single or multi-hop by using intermediate nodes that is act as routers for forward and relay messages.Because of infrastructure non-requirement facility,MANET instantaneous deployment will provide them for appealing in huge applications in various

domains like military operations and communication, fire and police services, rescue operations and emergency search, and inter vehicle networks, disaster recovery, PANs, virtual conference or classrooms setting, supporting nurses and doctors in hospitals, etc. Figure 1 depicts a typical communication scenario in MANET. MANETs routing design exhibits cooperative and distributed behaviour that makes it easier to target in DoS attacks [3].The purpose of DoS attacks is for preventing the users intended from processing the resources available and thereby the services. Intruders in MANETs will compromise easily mobile nodes, and DoS attacks are launched through these nodes that are compromised. DoS attack done by several nodes that are distributed in the network throughout is known as Distributed DoSattack. The DDoS attack is more dangerous and then difficult to address in real-time.

The DoS attack is categorized by two huge categories:vulnerability attacks (here vulnerability in target process is exploited) and then flooding attacks (invoking by the huge level of service requests/bogus traffic). The RREQ attack is a type of flooding DoS attack in which the malicious nodes will launch a huge level of packet route RREQ for IP addresses containing destinations for depleting resources computational and battery of intermediate nodes and these nodes will consume more energy. The flooding RREQ attack will affect significantly conductance of on demanding protocol routing, specifically DSR and AODV in MANETs,while the process of discovering route is triggered usually through broadcasting packets RREQ, and then flooding such RREQ bogus packets without any adhering for limiting rate in a network that leads for degradation to a severe extent in system throughput. Some protocols - SAODV, Ariadne,and then ARAN are vulnerable to flooding RREQ attacks in the same fashion. Essential workis done by researchers in detection development and then counteracting models against flooding RREQ attacks. However, existing models suppress a node because of the amount increased in packets RREQ in unusual situations and then failed for preventing the flooding RREQ attack at a decreased rate to destinations [4].Arecent study is an effective technique for suppressing the packets RREQ surplus at the single neighbour hop. This will consider the interval time approaches in the middle of the two successive packets RREQ that is evolved from this node for evaluating node status. Moreover, this model produces a better outcome only when interval time in the middle ofsuccessive packets RREQ is distributed uniformly, but it will mark inadvertently a node as black listed or grey listed because of the two successive packets RREQthat will be less within interval time other than a threshold that is predefined already.

For maintaining secure and reliable communication through MANETs against flooding RREQ attack, one idea based on trust,that will not only assist inidentifying node malicious, but also increase performance security and network robustness. The mobile node will support and trust each other mainly in normal network operation based on relationship trusted and that will establish bythe earlier setting of successful transactions in communication.Even several numeral solutions on security that depends on trusted management are presented in MANET.The present detection modelfor inhibiting flooding RREQ attack and then reduce blacklisting possibility of a node innocent because of increased RREQ packet amount in unusual situations [5]. Thus in several wireless networks, like ad hoc, delay-tolerant networks, and sensors, node destinations are identified from a source node througha process of flooding. Flooding efficiency is more important to nodes, they are driven througha limited battery. A simple scheme in flooding for transmitting an RREQ message depends on the power remaining of their node that does not utilize complex calculation and control packets. It initially shows node density limit which causes throughput decrease and then the scheme is superior in energy efficiency, including energy consumption and throughput. Next, flooding times numbers are made uniform, each node has the same time for replacing the battery. When a node is static, the lifetime will be longer than a conventional model.MANETis reliable and promising and finds utility in real-time applications such as military communication, traffic management,and in places while telecommunication does not reliable. One main application in MANET is Walkie-Talkies. Therefore preventing packet flooding will increase energy efficiency in MANETand also improve the packet delivery ratio, decrease end-to-end delay, and thereby capable of alleviating malicious nodes impact from a network.The remaining paper contains related works in section 2, proposed work in section 3. Section 4 contains experimentation findings followed by the conclusion in section 5.

2. RELATED WORKS

Existing method in the literature describes the comprehensive analysis and evaluation of two routing protocol classes that are optimized in MANET: proactive (OLSR,DSDV), and reactive (AODV, DSR). This protocol is designed particularly for MANETs nature of dynamic here node will move actively, nodes connections are broken regularly, and then reconstruct the path that is needed [6]. MANET is utilized in a large level of applications that includes military areas,rescue operations, and then oceanography. Moreover, the battery islimited in a node, and then typically, that will not cost-effective or applicable for replacing

the node battery. Other than this,network's dynamic nature thatwill lead to processing and then a requirement of rerouting, and then movements will speed up the depletion of the battery. So, routing protocols of energy efficiency will affect network performance significantly. The author makes a study on both classes in MANET, and then investigating many parameter's effects on network conductance by simulations excessively, and analyzing parameters variations as to how it affects its performance.

MANETs that are autonomous,self-configuring, and network with a type of infrastructure-less, that will associate for mobiles wirelessly have been elaborated in the literature [7]. Each device continuously varies its link with another device where as MANET will permit for autonomous move through any other path. The challenge in MANET is for avoiding congestion through information routing appropriately through facilitate routing which involving equipment for each device for constantly keeping needed information. Various protocols with their ability and assume degree fluctuate within space bounded that is assessed through different academic papers, and also with nodes with less hop for each other.Important variable such as average throughput,bandwidth, and success ratio of a packet, is attained after various simulations for numeral nodes and then make a comparison for evaluation performance. So, cluster-based energy balanced algorithm is utilized to MANET for mitigating a breaking common link and node optimization energy.

Another method in literature focused on mobility issues and also energy efficiency for developing a clustering design inspired through parallel finding a multi agent stochastic model of PSO. The CH election will make mobility care and then energy remaining and also connectivity degree to choose nodes for serving as CHs for longer time duration.The formation of a cluster is presented by taking the fitness function of multi-objective by using PSO. The author makes experiments extensively on the simulator NS-2 network and then compared them with another existing design [8] [9].The outcome makes effective in proposed design by life time network, energy consumption,packet ratio in delivery,an average numeral of formed clusters, and re-clustering needed.

A new multipath fault-tolerant routing protocol [10] is presented for reducing loss of packet because of breakage in routes, which utilizes a novel discovery route and mechanism for maintenance. And it also uses another route alternatively for retransmitting data whenever an intermediate node is not able for forwarding it, because of failure in link or node. The present protocol is simulated in NS2- network and evaluated for its performance by using packet drop and delivery ratio, end-to-end delay, energy consumption,and throughput by

changing pause time, flows number,and then traffic rate. This simulation outcome shows that the present protocol will out perform the works that are existing in the above metrics term.

An effective method [11]for a zone of efficient energy based on routing protocol is developed to decrease broadcasting redundant by an on-demand collision of parallel broadcasting that is guided. Nevertheless, storm broadcast is occurred because of simultaneous transmittingin guided collision broadcasting that causes more consumption of power. The authors deal with a new design to increase the zone ofefficient energy based on protocol routing that will control the topology network through node estimation rate out of the die. Moreover, the theory approach called a game with a zone of efficient energy depends on protocol routing for improving QoS routing in MANET.

Another method [12] explains the routing protocol efficiency based on packet delivery. Nevertheless, because of the battery's nature power tool in WSN and MANET network, the routing protocols power consuming is also considered for routing design betterment. Hence forth,energy efficiency applicability will become one of the main criteria that are used for evaluating performance. The author evaluates routing design performance for the architecture of MANET which is highly dense. The result is for presenting a new design based on a cluster with low energy consuming and evaluating improvements through current systems.

QoS and secured routing based on a multipath route energy in MANET [13] is proposed in the literature. For selecting a multipath route, the author proposed the PSO-GSA algorithm. By using this design,efficient energy multipath route is chosen in this network. After numeral transmission, routes will lose their quality of a link. So,the path is chosen optimally from routes established in a network by using an algorithm cuckoo search that will perform depends on cuckoos behaviour.

A novel detection design for flooding attacks in MANET depends on an approach called machine learning [14] is presented in the literature.The design relies on route information for every node for capturing the same characteristics and node's behaviours that are belonging to a similar class for deciding while it is a malicious node. The author also presents a novel preventing flooding attacks in a routing protocol through extending AODV protocol and then integrating the algorithm of FADA. The performance is evaluated by successfully detecting the attack ratio, and then routing load.The results based on FAPRP will detect 99% of flooding RREQ attacks inevery scenario.

Another method uses an increased AIF AODV protocol which will isolate and detect node flooding in a network. NS-2.35 is used for simulating and for proving the efficiency of the present model [15] [16].The outcome of an enhanced modelby End to End Delay, Throughput,PDF, NRL,and ARE is closer for AODV without any attack of flooding.

An effective method known as flooding attack mitigating mechanism is presented that will depends on the value of threshold dynamically and it contains three phases. And then it uses many special nodes known as F-IDS which are employed in MANET used for detecting and preventing flooding attacks [17].The node F-IDS is promiscuous for monitoring node behaviour.It also improves metrics of performance in the network regarding PDR, then throughput and decreases overhead routing and also routing load.

A belief based method [18]is used for detecting malicious nodes based on belief of node neighbour. The present approach simulation is conducted by using aNS- 2simulation. The DRRB application outcomes that it will effectively and efficiently detect an attack in flooding which is in MANET.

A novel method which depends on behavioural metrics of AODV that willbe used for detecting and preventin gattack of flooding in MANET by using SVM is also proposed in the literature [19]. The authorused a method called CO, PMIR and, PDER as metrics forflooding attacks prediction. The present method is applied on testbed NS-2.

An explanation related to several DoS attack types in MANET and with special emphasis on flooding is discussed in literature [20]. Flooding attack occurs in all on demanding protocol routing.The author presents a new technique for mitigating the RREQ effect of attack flooding in MANET by using function trust estimating in DSR.

3. PROPOSED WORK

This proposed work presents the classification, hybrid routing protocol that optimizes energy and prevent flood attack. For classifying,the ANFIS model is used. The hybrid technique ACO and FDR PSO are used in combination with the routing protocol SMA_2AODV model in the proposed work. Figure 2 depicts the proposed model flow in detail. MANET needs an approach named trade-off, either compromising flooding attack and energy efficiency or other metrics of a network like a delay, data rate, distance, etc.Optimization models are designed to concentrate on reducing trade-offs for supporting the growing population of a network. This proposed model concentrates on avoiding attacks for energy optimization and its related parameter of the network with the least compensation.

Further,SMA is integrated with the AODV protocol for detecting RREQ flooding attacks. This flooding attack is most dangerous because it will create broadcast storms easily and more energy consumed. Based on this model,novel agent SMA is used to avoid flooding attacks for increasing energy efficiency in MANET.

Using ANFIS, the nodes in the network are classified into trusted or non-trusted nodes based on theirbehaviour. If a node transmits more packets over a particular time then it is isolated and removed from the trust list. For that, a minimum threshold limit is set for each node. For example, if a node sends more than 2 of the same packets over a particular time then it can be a malicious node and it is removed from the trusted node list. Depending on that, the node list is created. This process is repeated for a particular time to identify malicious nodes. This present system contains training and classificationdistinct modes. In MANET, the featureis extracted from non-malicious and malicious nodes and these feature extracted is trained by neural network classifier. During classification, the feature obtained from a single node is classified w.r.to trained pattern for classifying the test node into non-malicious or malicious.

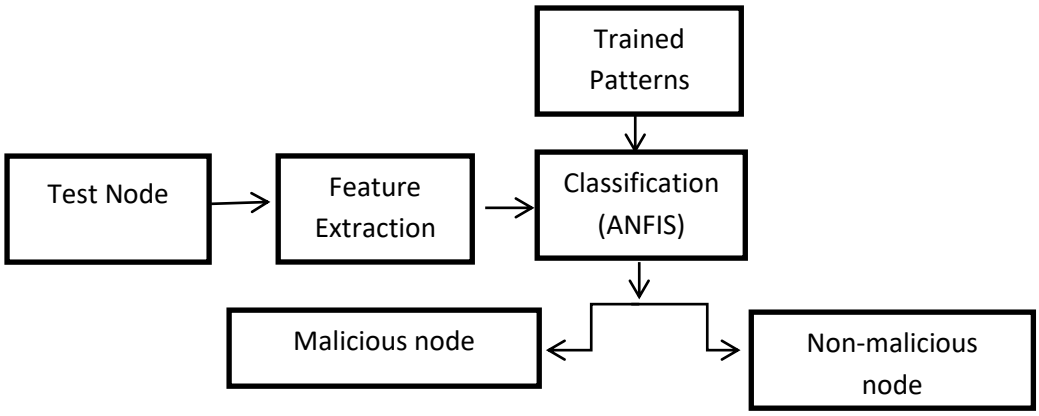

Fig.2Classification of malicious and normal nodes using ANFIS

The features extracted are fed into classifier input for the test node classification in MANET into malicious or non-malicious nodes. Figure 2 depicts the ANFIS classifier based node classification. The conventional classifier such as neural networks and SVM, which havemore latency for classification,will not suitable for network classification that consists of more nodes. So, a ANFIS classifier is utilized to node classify for their trust ability.

The output of the ANFIS classifier is given as (1),

$$C_j^5 = \sum_{j=1}^{2} \overline{w_J} f_j = \frac{\sum_{j=1}^{2} w_j f_j}{w_1 + w_2} \quad (1)$$

Malicious node is removed in MANET by detecting RREQ flooding attack for reducing more energy consumption of nodes. SMA$_2$AODV will perform by AODV protocol where each received RREQ packetis continued and accepted for broadcast for every neighbour. While comparing with AODV, SMA agentis used for collecting data for calculating minimal system time-slot ($STmin$).

SMA contains two stages, namely training, and checking. Where, after training is completed, checking is performed. In the trainingstage, each nodewill collect information of other node's route discovery in the system while receiving the RREQ request package to build up a system time-slotdiagram.

In this, discovery time of route is calculated by (2) in which e and d is the time-point of route discovery and route response is received.

$$s = d - e \quad (2)$$

RDTS is the duration between two discovery and it is calculated by 3 in which $d_i$is the receiving route time-point of i, $e_{i+1}$is the route discovery time-point which is started.

$$S = e_{i+1} - d_i \quad (3)$$

In the AODV protocol, nodes route discovery frequency is compuated based on how the node frequently finds a route for the needed destination. Every normal node within a range hasroute discovery frequencies, but malicious node has more route discovery frequencies because their aimis for network flooding and it consumes more energy.

Minimal route discovery single node and system time-slot is calculated by 4, 5 where *n, m* is the time-slot and network node number.

$$Smin = Min(Si); \forall i = \overline{1..n} \quad (4)$$

$$STmin = Min\left(S_{min}^{j}\right); \forall j = \overline{1..m} \quad (5)$$

The NS2 version 2.35 is used for building a training dataset of normal (NVC) and malicious (MVC) vector classes.Every normal nodewill collect the source node's route discovery data in the network. Whilethe RREQ packet is received, a node will employ the route discovery frequency vector and utilizesa machine learning designfor determiningwhether the source node is malicious or normal. The kNN-classifier is used for classifying the two classes depend on the route discovery frequency vectors for MVC or NVC.In kNN, the neighbour nearest is referred to as a distance of two samples, and different distance metrics are used depends on the feature vector which represents the samples. The Euclidean in (6) to calculate the V1 and V2 distance.

$$v(D_1, D_2) = \sqrt{\sum_{j=1}^{m}(D_1[j] - D_2[j])^2} \qquad (6)$$

After completion of the training stage, every node will checkthe RREQ packet security received from other source nodes N_a. If the time-slot of route discovery node $N_a$is lower than the system minimal time-slot (S<STmin), then a flooding attack has appeared, N_a adds N_b into Black List. Every RREQ nodes packets in Black List are dropped without checking security needed to enhance processing and energy efficiency.Thus,it identifies whether the source node is a normal node or malicious and preventing flooding attacks will decrease energy consumption.

Once the trusted nodes are identified, routing is established through ACO and FDRPSO hybrid model that is integrated. ACO will be enhancing node life time by using duty cycle design and FDRPSO will optimize node consumption of energy.The aim of ACO design is to optimizing Residual Energy(RE). The greater residual energy node is takenfor transmission depends on the algorithm of the duty cycle.Initially, ACO will select energy effective route for transmitting data between a source node and the destination node by visiting the node intermediated between them. After the ant traversalcompletion, with every visitedhop, updatingon pheromone values is made. After 'c' transmissions,for each node visited, ACO updates residual energy. The ant set is attracted with higher pheromone links and a node of residual energy. The active node moves to the sleep state and the sleep node moves to the currently active state.

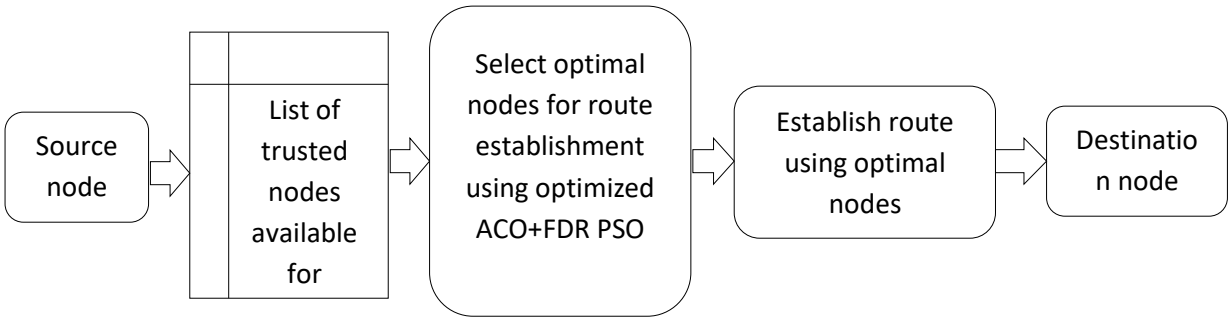

Fig. 3 Hybrid energy-efficient routing to avoid flooding attacks (HEERP)

Pheromone value is referredto asant visiting node residual energy. The ant probability 'c' choosing 'm' node from 'n' at a specific timet is observed by equation

$$P_{nm}^{c}(t) = \frac{[\tau_{nm}(t)]^{\alpha}.[\mu_{nm}]^{\beta}}{\sum_{l \in N_n^c}[\tau_{nl}(t)]^{\alpha}.[\mu_{nl}]^{\beta}} \quad if\ m\ \in N_n^c \qquad (7)$$

Where, P_{nm}^{c}-is the node probability misselected by ant from node nτ_{nm}- intensity of pheromone, N_n^c- nodes set and μ_{nm}=RE Heuristic value is available.

The Node residual energy is given by Eq.(8)

$$RE = E_i - E_j \quad (8)$$

Where E_i- initial energy.

The updated pheromone values by ants are given by equation (9)

$$\tau_{nm} \leftarrow (1-\sigma).\tau_{nm} + \sum_{i=1}^{j} \Delta\tau_{nm}^{i} \quad (9)$$

Where σ–is a rate of evaporation, j –ants numberand $\Delta\tau_{nm}^{i}$- pheromone link (n,m) by the ith ant.

$\Delta\tau_{n,m}^{i} = \frac{1}{H_i}$If ant i travels on its link n, m.

Where $H_i$is ith ant hop count.

When ant returns to the source node, the information is updated about the visited path. And more antsare deployed randomly to visit every neighbour path, source knows about multipath to the node destination. Figure 3 depicts hybrid energy-efficient routing to avoid flooding attacks. The optimal path is selected based on its higher values of pheromone and then ACO will pass the set solution to FDRPSO.

FDR PSO will optimize energy in the pathselected by ACO. This process is done in multipath for consumption of energy. Successive energy effective route is selected for data transmission. PSO convergence issue is protected in FDR PSOby takingi_{best}a particle that maximizes energy fitness distance ratio is given by Eq. (10)

$$\frac{E_d(P_n) - E_d(X_n)}{|P_{nc} - X_{nc}|} \quad (10)$$

Where, $E_d(P_n)$ is the particle energy consumed in the best position, $E_d(X_n)$ is the particle energy consumed in the present position, P_{nc} is the particle best position and X_{nc} is the current position.

The particle velocity is updated byEq. (11)

$$V_{nc}^{L+1} = (w.V_{nc}^{l}) + a_1 s_1 (P_{nc} - X_{nc}) + a_2 s_2 (P_{gnc} - X_{nc}) + a_3 s_3 (P_{ic} - X_{nc} \quad (11)$$

Similarly, particle position is updated by Eq 12.

$$X_{nc}^{l+1} = X_{nc}^{l} + V_{nc}^{l+1} \quad (12)$$

Where, P_{nc}, P_{gnc}arepbestand gbest particle (best previous and global best position), X_{nc} and V_{nc} are the current position value andnth particle velocity, the acceleration co-efficient are a_1, a_2, a_3, s_1, s_2, $s_3$are the random numbers in the middle of 0and 1, w is the weight of inertia.

From the above equation, energy efficiency and classification into normal or malicious nodes for preventing flooding attacks in MANET is performed in this proposed approach. The pseudo-code for the proposed technique is summarized as follows.

Algorithm: Energy-efficient and Flooding attack

Input: n number of nodes

Output: Malicious or Non-malicious node

Start

Step.1 Classification(ANFIS) the nodes using Eqn.(1)

Step.2 Classifies normal node or malicious

Step.3 SMA$_2$AODV removes malicious node by detecting RREQ flooding attack

Step.4 Estimate minimal route discovery time-slot of all nodes using Eqn.(4)

Step.5 Estimate route discovery time-slot of the system using Eqn.(5)

Step.6 Build ant solution based on RE by duty cycle using Eqn.(7)

Step.7 FDRPSO starts depends on the ACO path generated and compute energy

Step.8 Choose particle of Gbest, Pbest, and Nbest for thepresent iteration

Step.9 Update every particle position and velocity using Eqn.(11) and (12)

Step.10 An energy-efficient path is obtainedby avoiding flooding attacks

End

4. RESULTS AND DISCUSSION

The proposed methodology for the detection of malicious nodes in the MANET is simulated in NS2 as the environment of simulation. The simulation settings are listed in table 1 shown below.

Table 1 Simulation Settings – Proposed Hybrid Routing Model (HEERP)

Network Simulation	**Range**
Routing Protocol	HEERP (SMA$_2$AODV +FDRPSO)
Network Size (m^2)	500 * 500
Transmission Range(m)	150

Network Simulation	Range
Number of Nodes	20
Packet Size (byte)	512
Simulation Time **(s)**	50
No. of attack nodes	5
Mobility Model	Random Way-Point
Velocity **(**m/s**)**	10
Pause Time	1 s
Initial Energy (mAH)	0.5

The performance of the presentdesign is comparedwith other algorithms and traditional AODV by throughput, and packet delivery ratio, energy, and detection ratio. The other methods include the conventional AODV, energy-efficient secured routing protocol (SSRP) [22], and Secure Source anonymous message authentication scheme (SAMAS) [21]. Generally, when node number increases, the malicious and non-malicious node number and energy consumption amount will also increase that drains the node's energy at faster rates. This model reduces unnecessary drain of energy due to flooding attack which is prevented by the SMA2AODV protocol. The ACO-FDRPSO model will help successive nodes to data transmission that is selected by current active nodes set that helps in preserving the node energy. Therefore the proposed system hashigher residual energy than the other existing approaches.

Throughput

Throughput is known as the total packets number transmitted successfully to the node destination over aspecifictime. Its range varies from 0 to 100 and it is calculated in bits per second.If the node number is less, then the throughput is high and the proposed system performance will behigh and if the node number is more,then the throughput is low and the performance is low. It shows the proposed system performance analysis in MANET with resepect to throughput. Results show that the proposed algorithm has the highest throughput even under attacks compared with the other designsin highnode number results in the enhanced transmission of data between a source node and destination node that improves throughput.End- End delay is known as the average time required for a packet that can be

transmitted from the source to the destination node in the network.Comparative of Throughput & End- End delay is shown in table 2.

Table 2 Comparative analysis of Throughput & End- End delay

Parameters	Proposed [HEERP]	SSRP [22]	SAMAS [21]	Conventional AODV
Transmission throughput	1012kbps	646kbps	602kbps	550kbps
Receiver throughput	1049kbps	770kbps	780kbps	612kbps
End- End Delay (s)	0.54	0.79	0.81	1.2

Packet Delivery Ratio

Packet delivery is known as the ratio between the total numeral of packets lostover aparticular time and the total numeral of packets produced in a particular node. It is calculated in percentage and varies between 0 & 100. The system performanceis inversely proportional to the average packet loss ratio. If node number is less, its average packet loss ratio is low and the proposed system performance is high and when node number is more, its average packet loss ratio is high and the proposed system performance is low. It shows the proposed system performance analysis in MANET w.r.to average packet loss ratio. The RREQ Flooding attack will cause an impact on route discovery source node ability hence the sending packet ratio has been reduced.Among the other methods, ACO-FDRPSO is founded as successful for delivering more packets number to the correct node destination due to prolonged lifetime depends on neighbour selection.

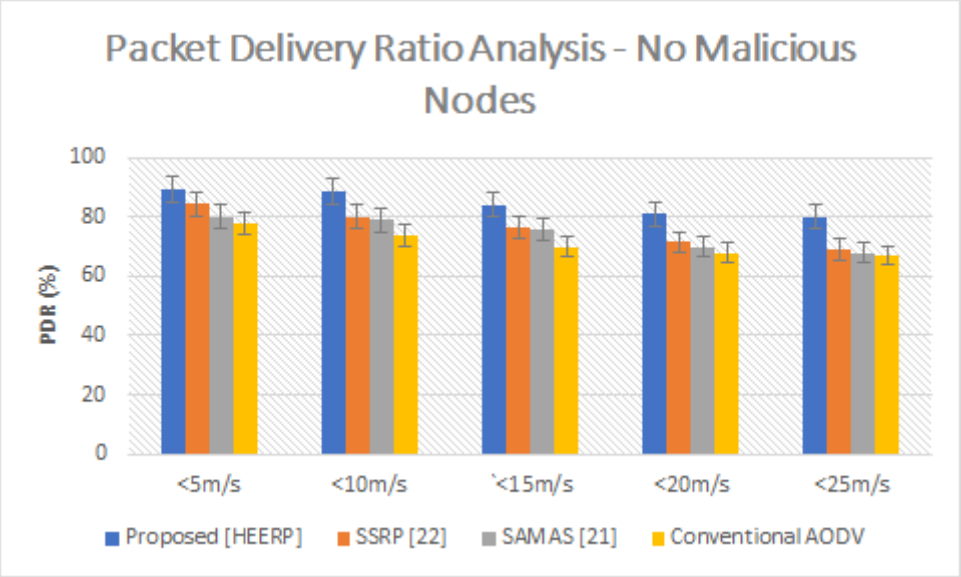

Fig. 4 Performance of PDR – Case I – No malicious nodes

The outcome in Figure 4 depicts the packet delivery ratio analysis with the mobility speed of <5m/s, <10m/s, <15m/s, <20m/s and <25m/s. No malicious node floods in case I.

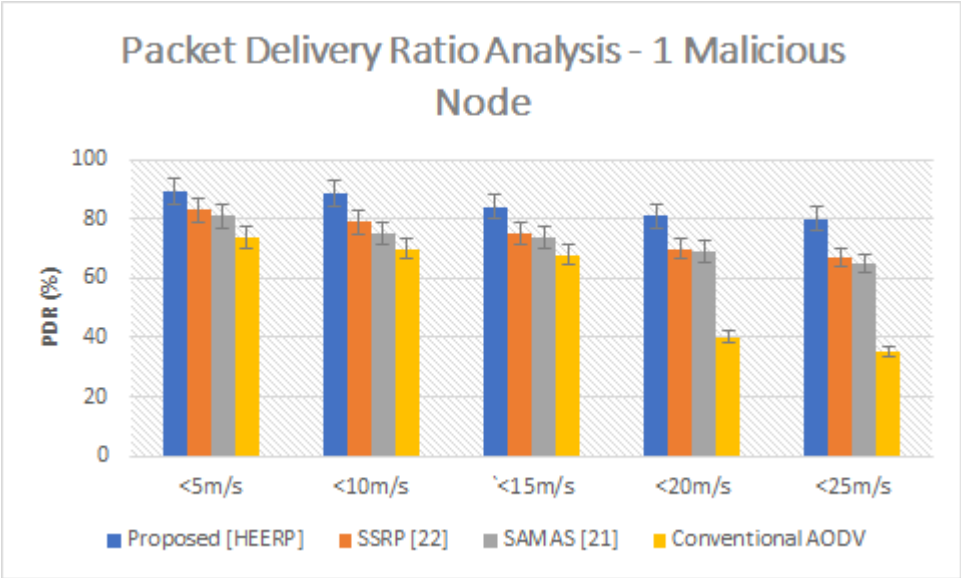

Fig. 5 Performance of PDR – Case II – One malicious node (5 packets/s)

Figure 5 shows analysis of packet delivery ratio with the high speed of <5m/s, <10m/s, <15m/s, <20m/s and <25m/s. Single malicious node floods 5 packets/s in case II.

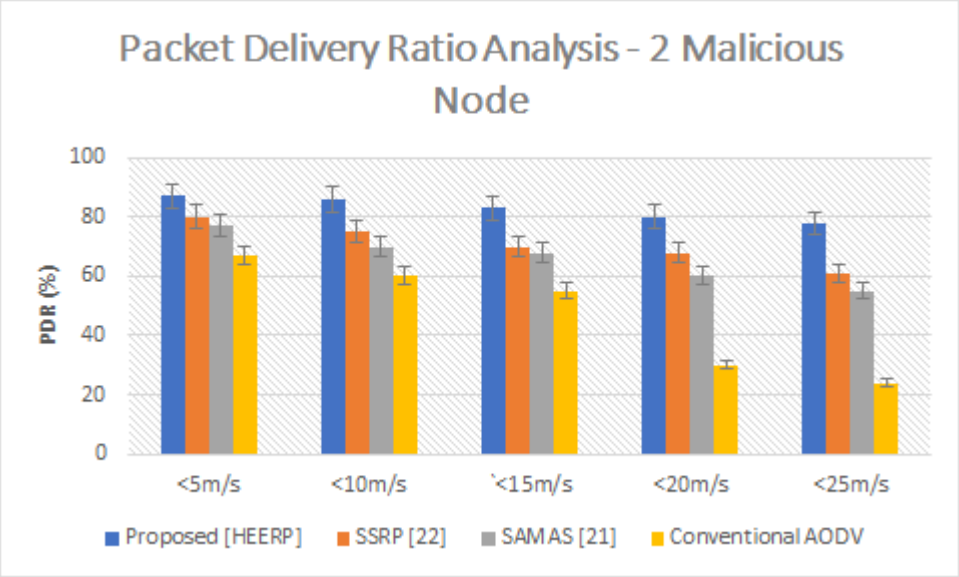

Fig. 6 Performance of PDR – Case III – Two malicious node (10 packets/s)

Figure 6 depicts PDR performance with the maximum speed of <5m/s, <10m/s, <15m/s, <20m/s and <25m/s. In case III, each of two malicious nodes floods 10 packets/s.

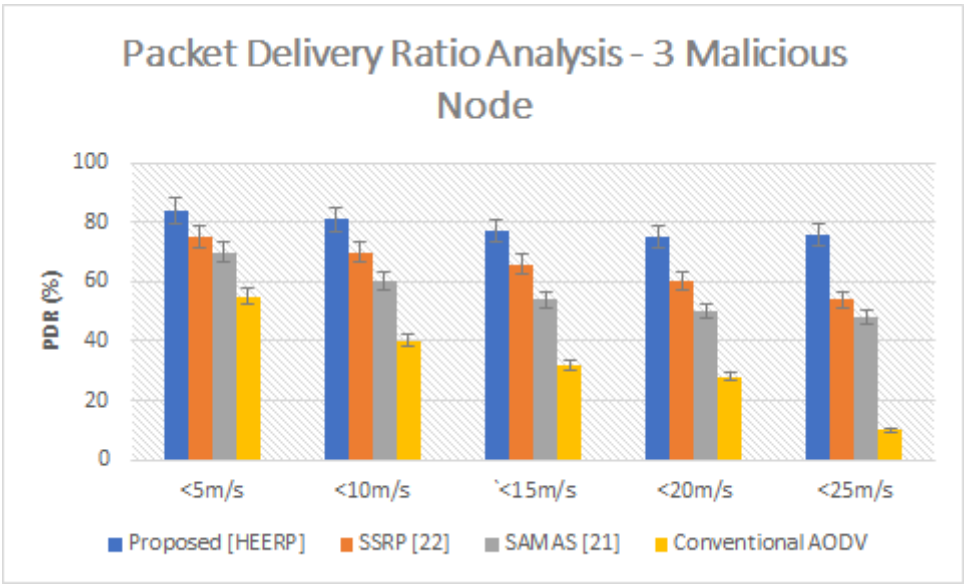

Fig. 7 Performance of PDR – Case IV – Three malicious node (10 packets/s)

Figure 7 shows PDR analysis with the speed of <5m/s, <10m/s, <15m/s, <20m/s and <25m/s. In case IV, each of three malicious nodes floods 10 packets/s. It could be observed in all case scenairos, that optimal performance is exhibited by proposed HEERP as compared to existing models

Detection ratio

Detection is known as the ratio between node numbers detected correctly to the total nodes number. Detection ratio is categorized as a node of malicious and non-malicious detection ratio. It is also calculated in percentage and varies between 0 & 100. The system performance is directly proportional to them alicious and non-malicious detection rate. The proposed system performance is high if itshigh detection rate and the proposed system performance will be low if its average packet loss ratio is low. It shows the proposed system performance analysis in MANET w.r.t detection ratio. When malicious nodes number is more, detection ratio is low and if malicious nodes number is less,detection ratio will be high. In MANET malicious nodes will consume high energy than other trusty nodes. The proposed methodology energy consumption in the MANET environment is illustrated. It shows that the SMA2AODV protocol will operate effectively when it suffers from RREQ Flooding attacks. After simulation, the detection ratio of fake RREQ packets is made successful in network topology.

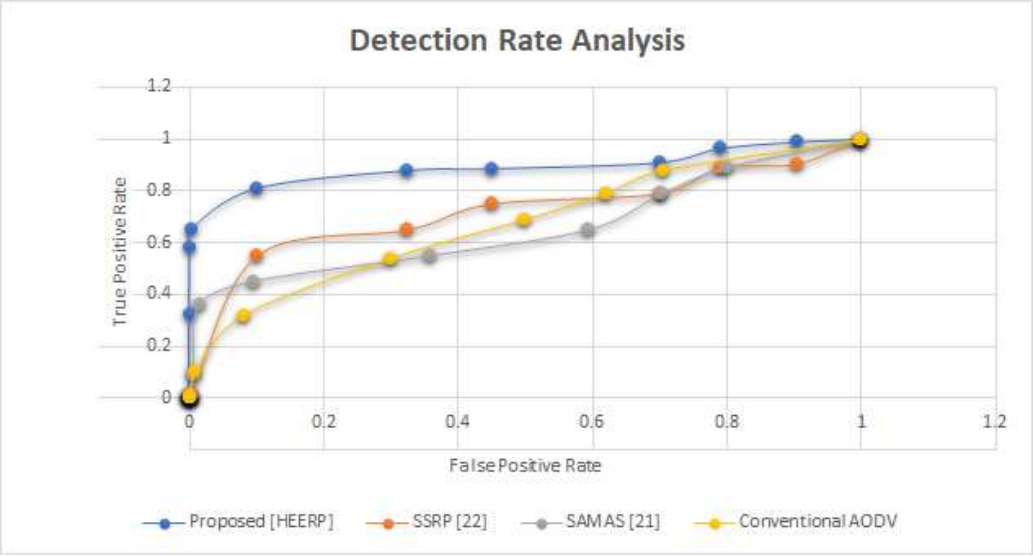

Fig. 8Detection Rate analysis – Packet Flooding attacks

The detection rate that is true and false positive rate is analyzed. Figure 8 depicts an analysis of the Detection rate of packet flooding attacks

Energy Consumption Analysis

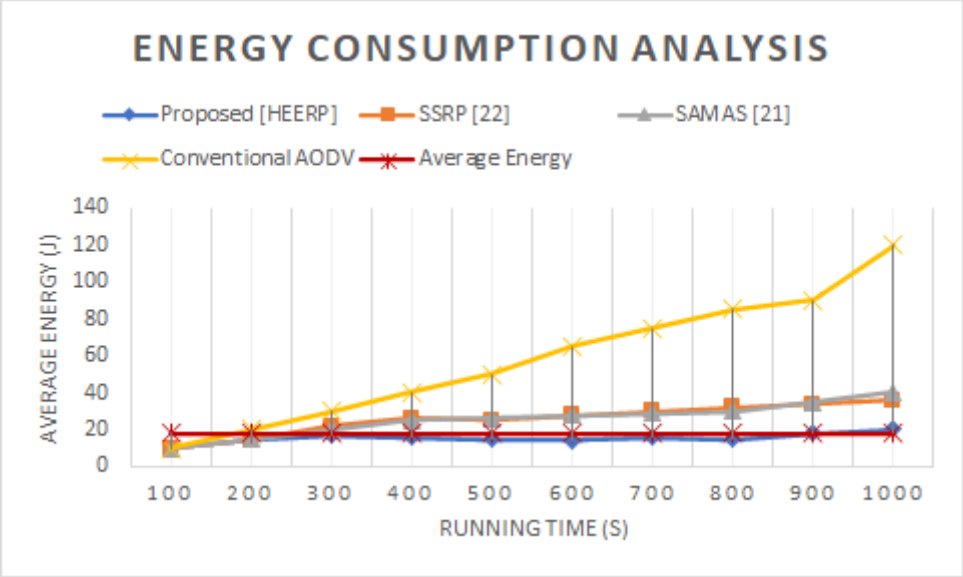

Fig.9Energy Consumption Analysis

The simulation result proves that by preventing flooding attacks energy efficiency is improved by using this proposed model. Figure 9 shows the average energy consumed with running time.

5. CONCLUSION

Malicious nodes will affect the efficiency of the nodesin the environment of MANET. These nodes are generated by the external attacks in MANET. This proposes an effective methodology ANFIS classifier to detect the malicious nodes in the MANET environment. The proposed system achieves improved throughput, average packet loss ratio and malicious node detection rate, and average accuracy. Security routing SMA2AODV protocol is integrated and operated effectively in the attacked topology of the network. The performance has been compared with other algorithms where the fake RREQ packets detection ratio successfully exhibited in network topology for the proposed HEERP.In MANETs energy optimization is a tedious task as the node's energy is limited whereas communication relies on the battery power availability. Through this proposed approach by preventing flooding attacks, ACO choosesan energy-efficient route and FDRPSO optimizes all nodes that are energy consumed. The hybrid ACO-FDR PSO optimization approach will consider energy as its function of fitness.The proposed design shows better throughput,packet delivery ratio, packet drop, residual energy, and SMA2AODV routing load become good when it is operated under RREQ attacks network topology. In the future, this work is extended for

detecting the residual nodes and for mitigating the other flooding attack effects in the MANET environment.

Declarations:

We, confirm that this work is original and has not been published elsewhere nor is under consideration for publication elsewhere.

Funding:

Not applicable

Conflicts of Interest:

Not applicable

Availability of data and material:

Not applicable

Code availability:

Not applicable

REFERENCES

1. Abu Zant, M., & Yasin, A. (2019). Avoiding and Isolating Flooding Attack by Enhancing AODV MANET Protocol (AIF_AODV). *Security and Communication Networks*, *2019*.
2. Agrawal, N., & Dwivedi, U. (2017). Improved Route Reliability to Overcome Route Flooding Attack in MANET. *International Journal of Computational Intelligence Research*, *13*(5), 1345-1354.
3. Boddu, N., Vatambeti, R., &Bobba, V. (2017). Achieving Energy Efficiency and Increasing the Network Life Time in MANET through Fault Tolerant Multi-Path Routing. *International Journal of Intelligent Engineering and Systems*, *10*(3), 166-172.
4. Gaikwad, S. S. (2018). Detection and Prevention of Flooding Attack in MANET using Support Vector Machine (SVM).
5. Gurung, S., & Chauhan, S. (2018). A novel approach for mitigating route request flooding attack in MANET. *Wireless Networks*, *24*(8), 2899-2914.

6. Jayavenkatesan, R., &Mariappan, A. (2017). Energy efficient multipath routing for MANET based on hybrid ACO-FDRPSO. *Int. J. Pure Appl. Math*, *115*(6), 185-191.
7. Kasthuribai, P. T., & Sundararajan, M. (2018). Secured and QoS based energy-aware multipath routing in MANET. *Wireless Personal Communications*, *101*(4), 2349-2364.
8. Khatoon, N. (2017). Mobility aware energy efficient clustering for MANET: a bio-inspired approach with particle swarm optimization. *Wireless Communications and Mobile Computing*, *2017*.
9. Kumar, S., & Dutta, K. (2017). Direct trust-based security scheme for RREQ flooding attack in mobile ad hoc networks. *International Journal of Electronics*, *104*(6), 1034-1049.
10. Luong, N. T., Vo, T. T., & Hoang, D. (2019). FAPRP: A machine learning approach to flooding attacks prevention routing protocol in mobile ad hoc networks. *Wireless Communications and Mobile Computing*, *2019*.
11. Muthurajkumar, S., Ganapathy, S., Vijayalakshmi, M., & Kannan, A. (2017). An intelligent secured and energy efficient routing algorithm for MANETs. *Wireless Personal Communications*, *96*(2), 1753-1769.
12. NS, S. F., Sharma, V. K., & Jain, A. An optimized Energy efficient cluster based routing in MANET.
13. Pandikumar, T., & Desta, H. (2017). RREQ flooding attack mitigation in MANET using dynamic profile based technique. *International Journal of Engineering Science*, *12700*.
14. Rajesh, M. V., Gireendranath, T. V. S., & Murthy, J. V. R. (2017). A novel energy efficient cluster based routing protocol for highly dense MANET architecture. *International Journal of Computational Intelligence Research*, *13*(5), 719-744.
15. Saraswathi, R., & Subramani, A. (2017). Performance Analysis Of Cluster Based Energy Efficient Routing Protocols For MANET. *i-Manager's Journal on Information Technology*, *7*(1), 12.
16. Selvi, P. T., &GhanaDhas, C. S. (2019). A novel algorithm for enhancement of energy efficient zone based routing protocol for MANET. *Mobile Networks and Applications*, *24*(2), 307-317.
17. Shandilya, S. K., &Sahu, S. (2010). A trust based security scheme for RREQ flooding attack in MANET. *International journal of computer applications*, *5*(12), 4-8.

18. Tu, V. T., & Ngoc, L. T. (2017). Sma 2aodv: Routing protocol reduces the harm of flooding attacks in mobile ad hoc network. *Journal of Communications*, *12*(7), 371-378.
19. Vu, Q., Hoai, N., &Manh, L. (2020). A Survey of State-of-the-Art Energy Efficiency Routing Protocols for MANET.
20. Yamazaki, S., Abiko, Y., & Mizuno, H. (2020). A Simple and Energy-Efficient Flooding Scheme for Wireless Routing. *Wireless Communications and Mobile Computing*, *2020*.
21. Ren, J., Li, Y., & Li, T. (2010). SPM: Source privacy for mobile ad hoc networks, Hindawi Publishing Corporation. EURASIP Journal on Wireless Communications and Networking, 2010, 5. doi:10.1155/2010/534712.
22. Singh, T., Singh, J. & Sharma, S. (2016). Energy efficient secured routing protocol for MANETs. Wireless networks. 23: 1001 – 1009.

Figures

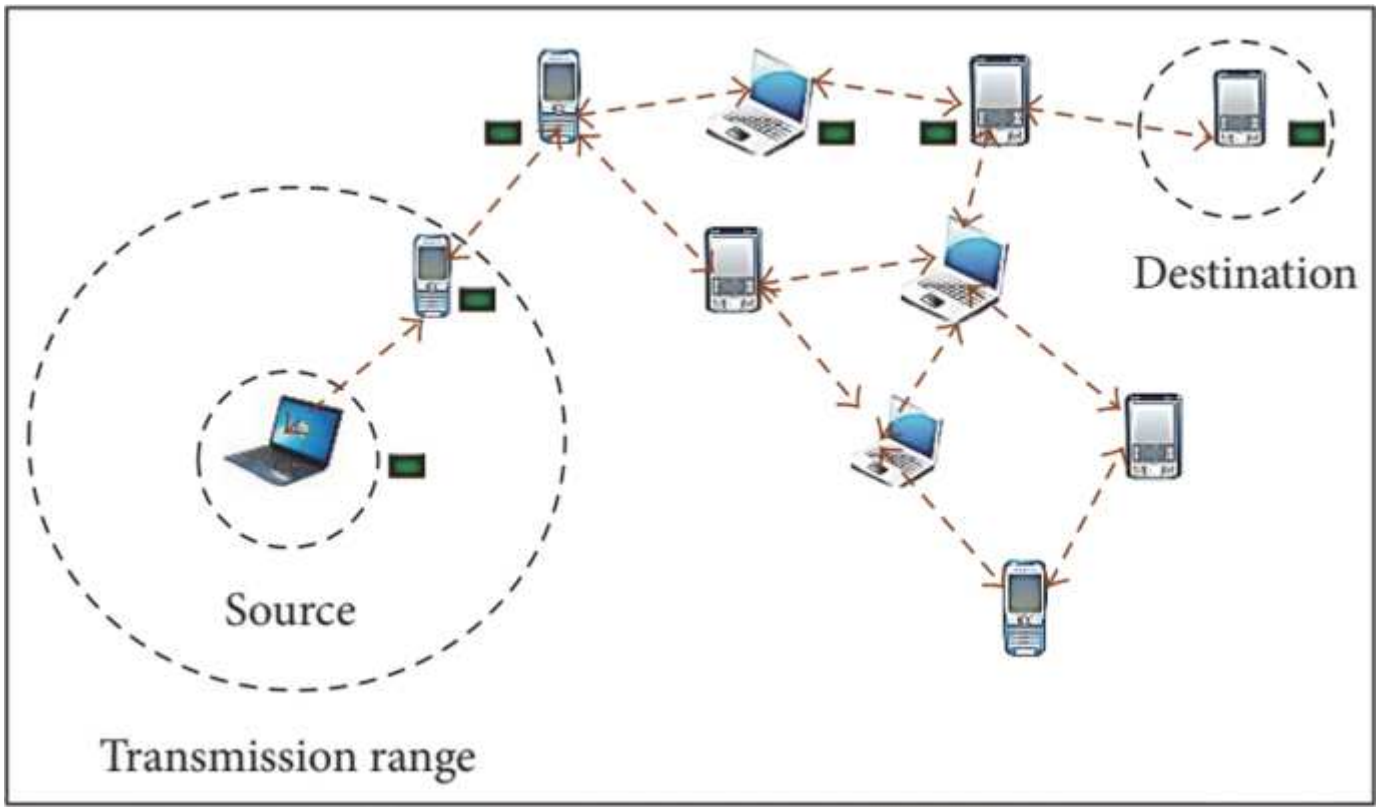

Figure 1

MANET architecture scenario

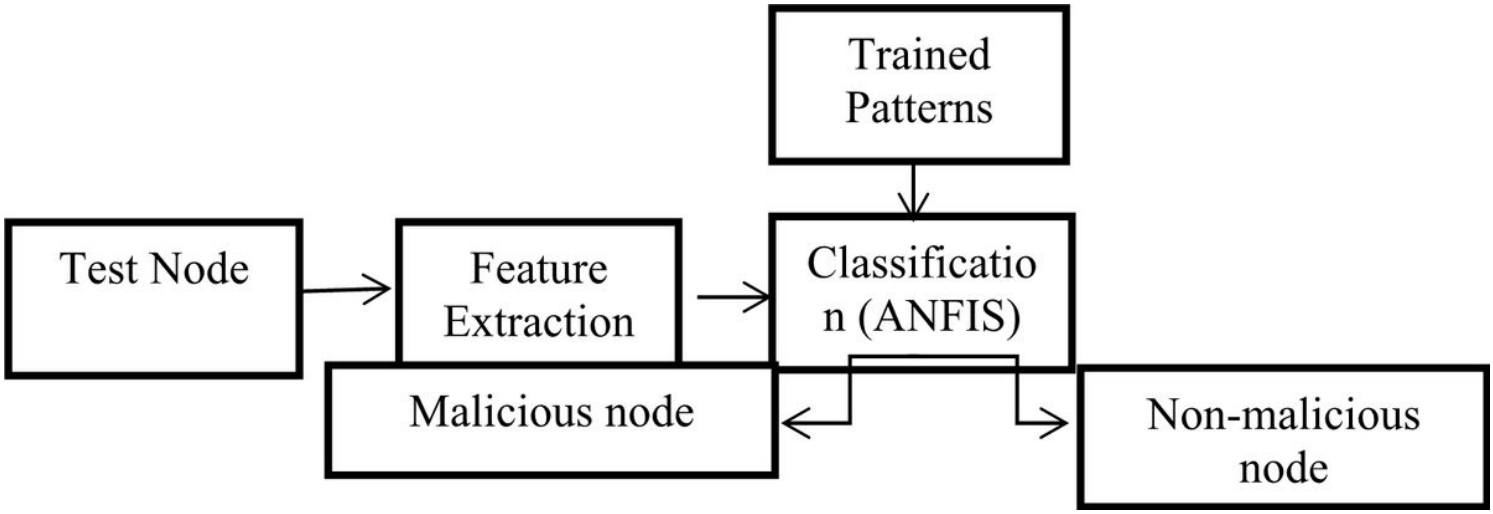

Figure 2

Classification of malicious and normal nodes using ANFIS

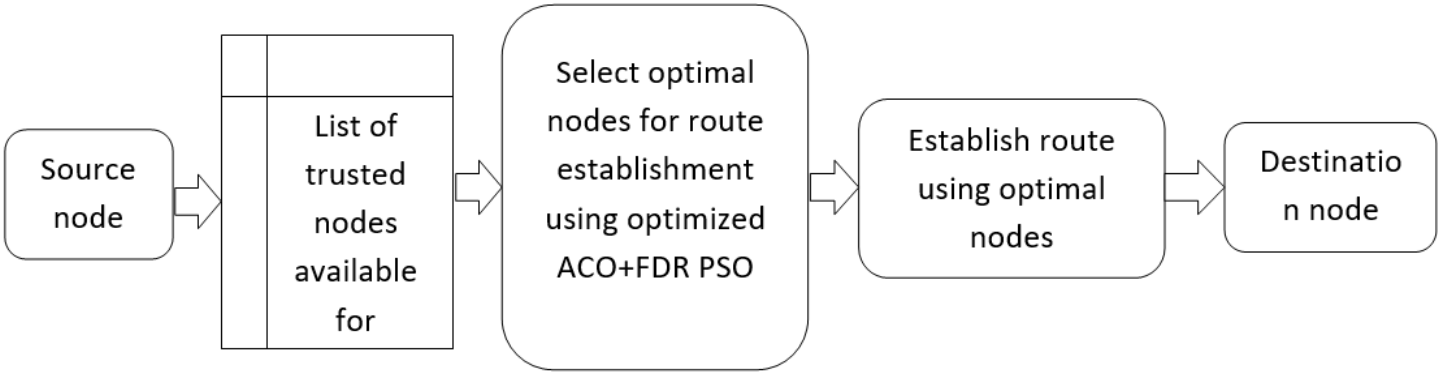

Figure 3

Hybrid energy-efficient routing to avoid flooding attacks (HEERP)

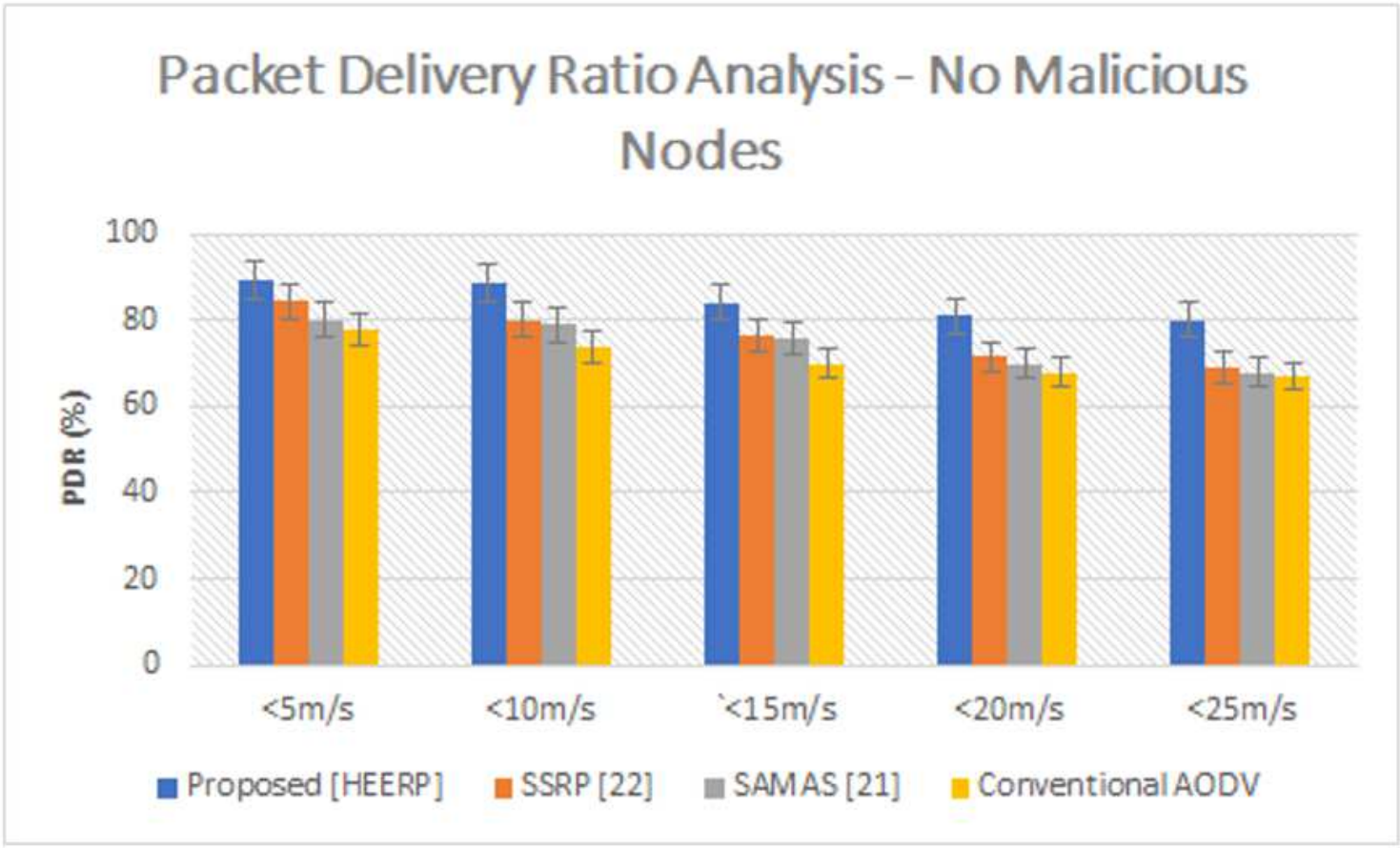

Figure 4

Performance of PDR – Case I – No malicious nodes

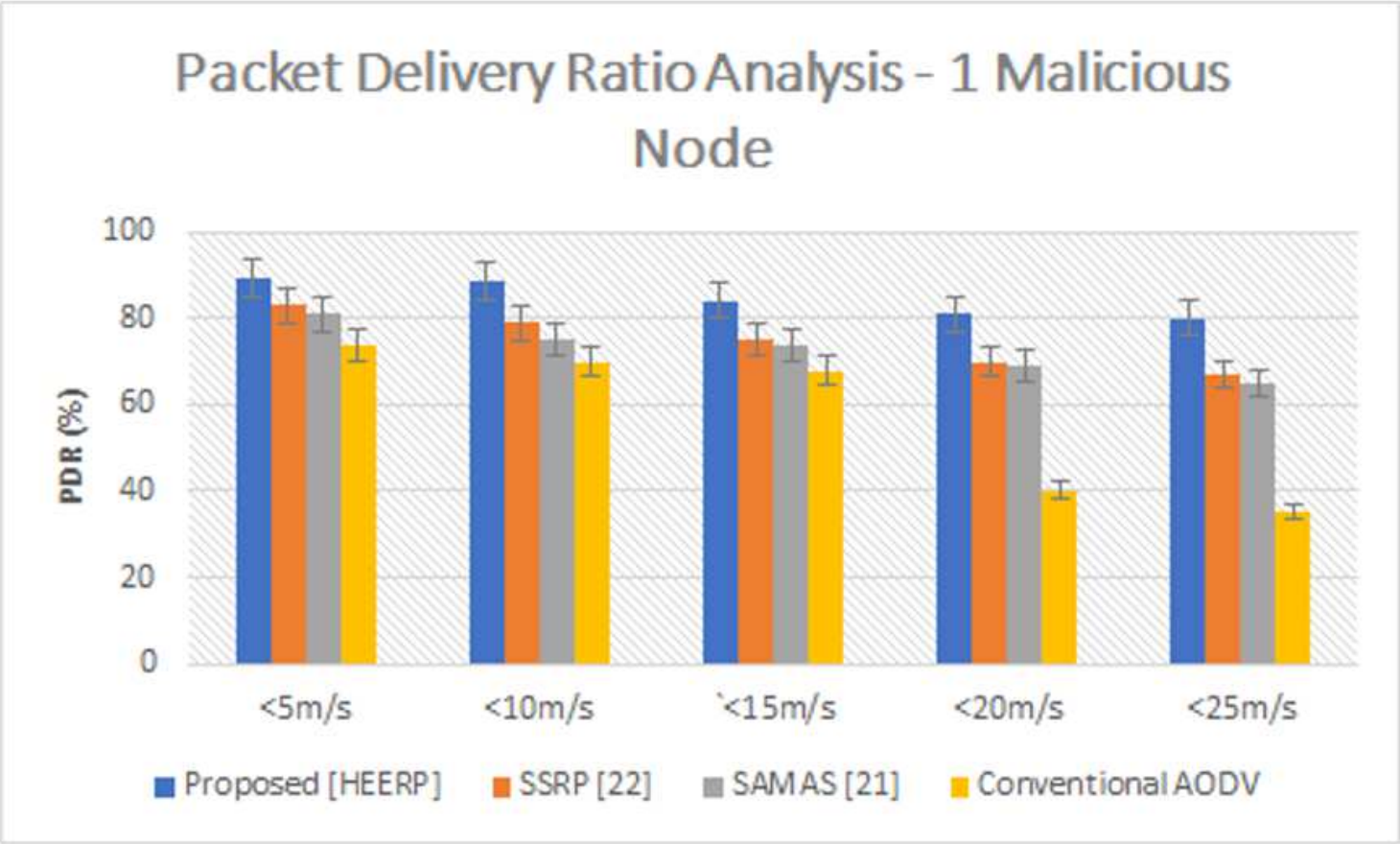

Figure 5

Performance of PDR – Case II – One malicious node (5 packets/s)

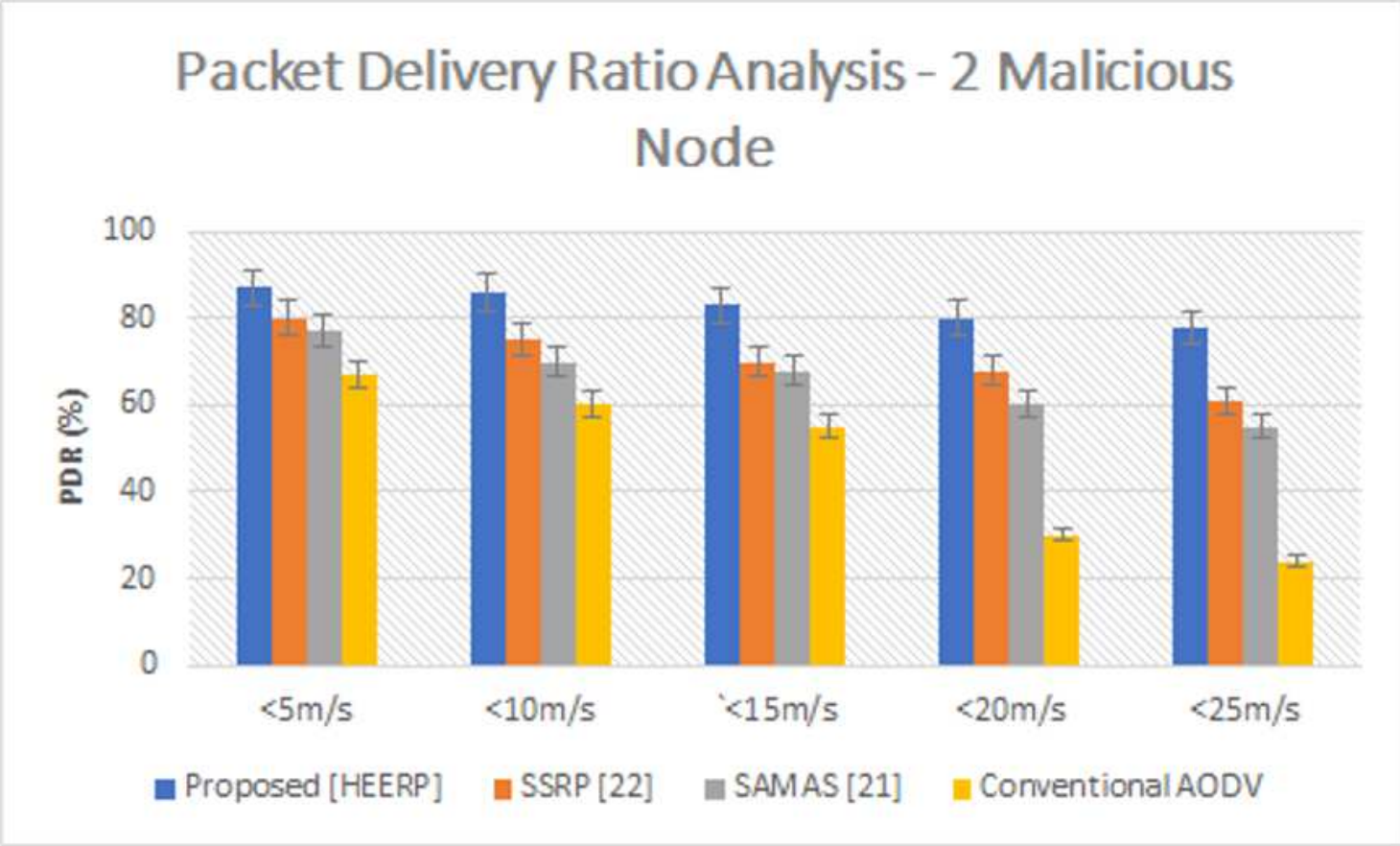

Figure 6

Performance of PDR – Case III – Two malicious node (10 packets/s)

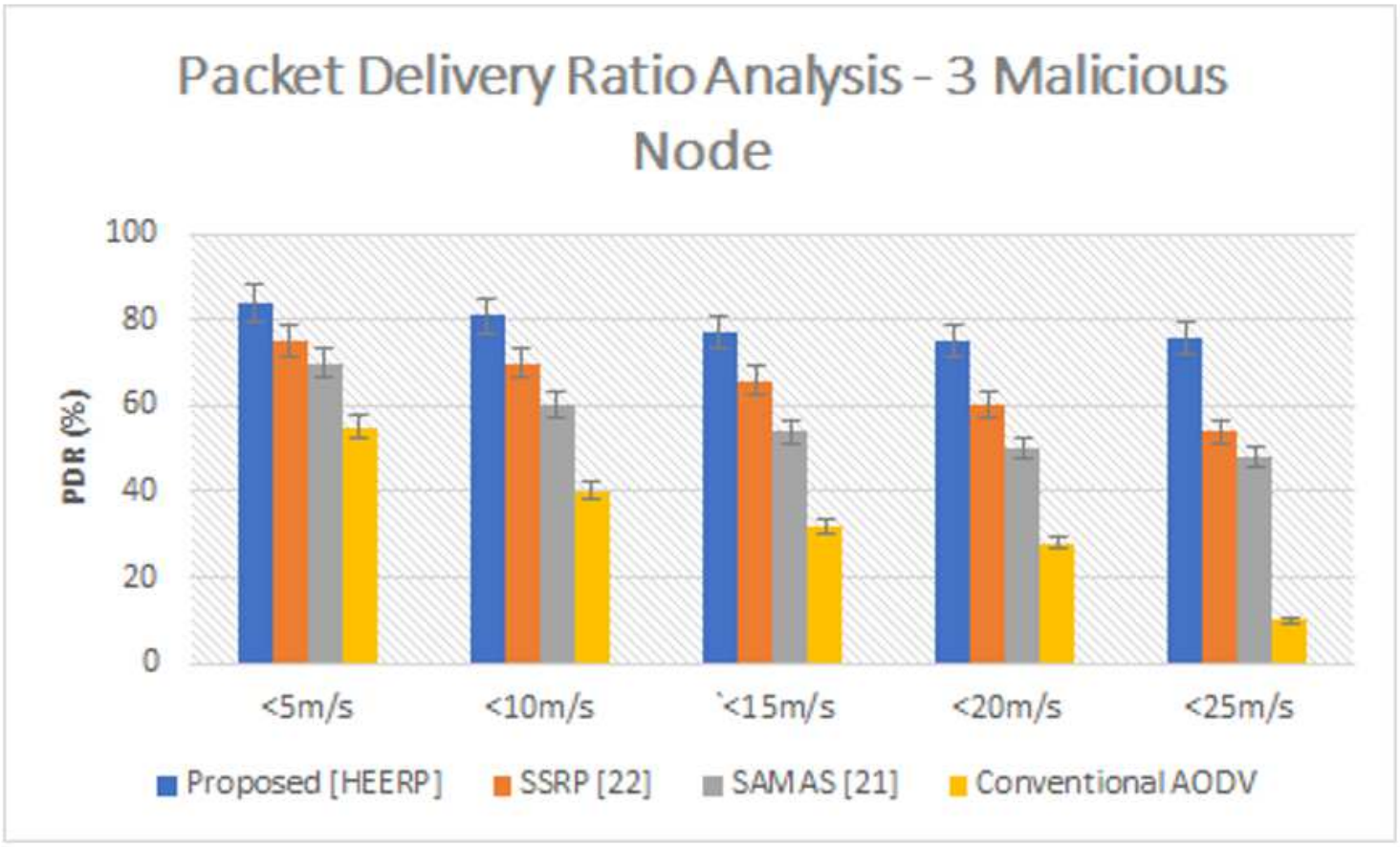

Figure 7

Performance of PDR – Case IV – Three malicious node (10 packets/s)

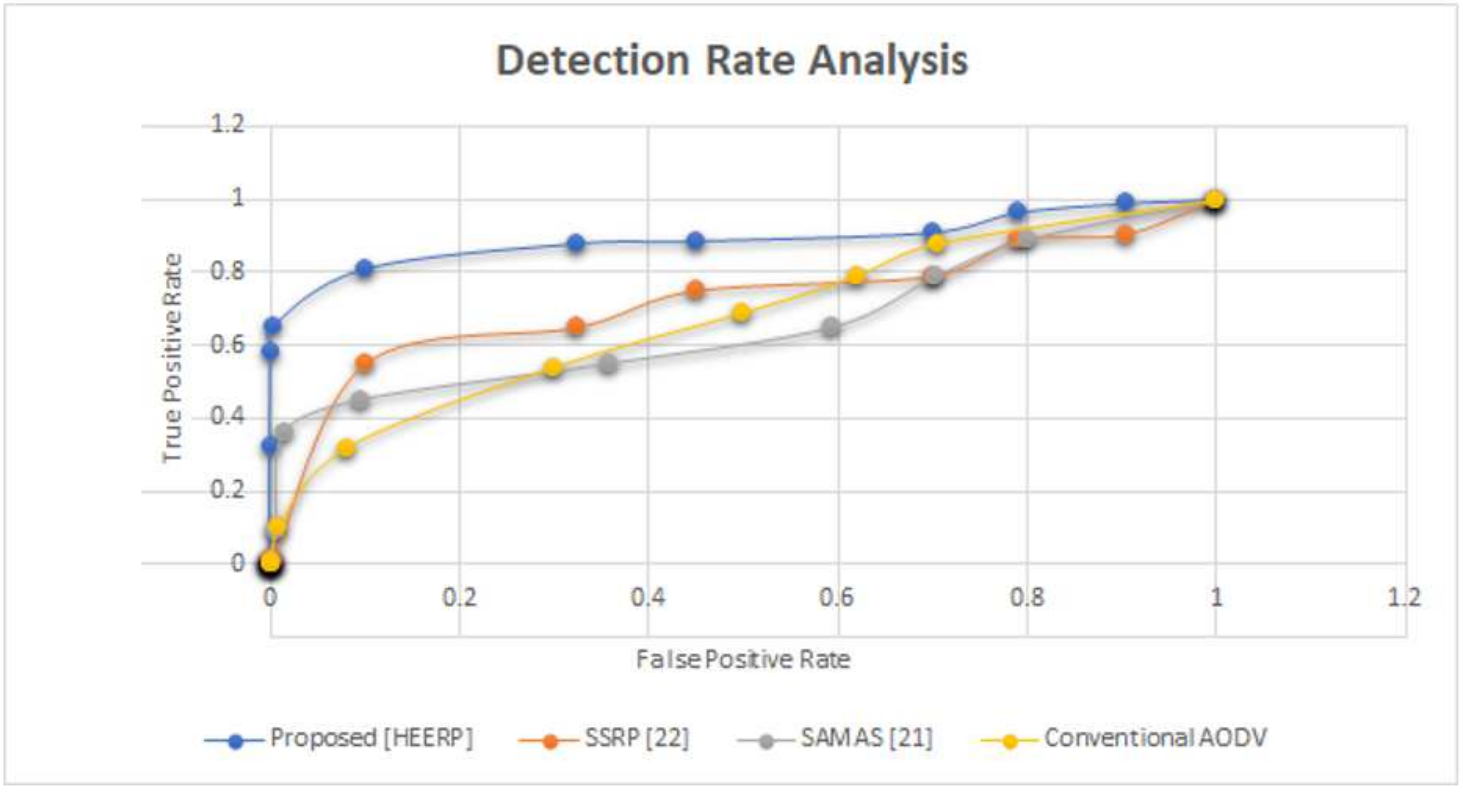

Figure 8

Detection Rate analysis – Packet Flooding attacks

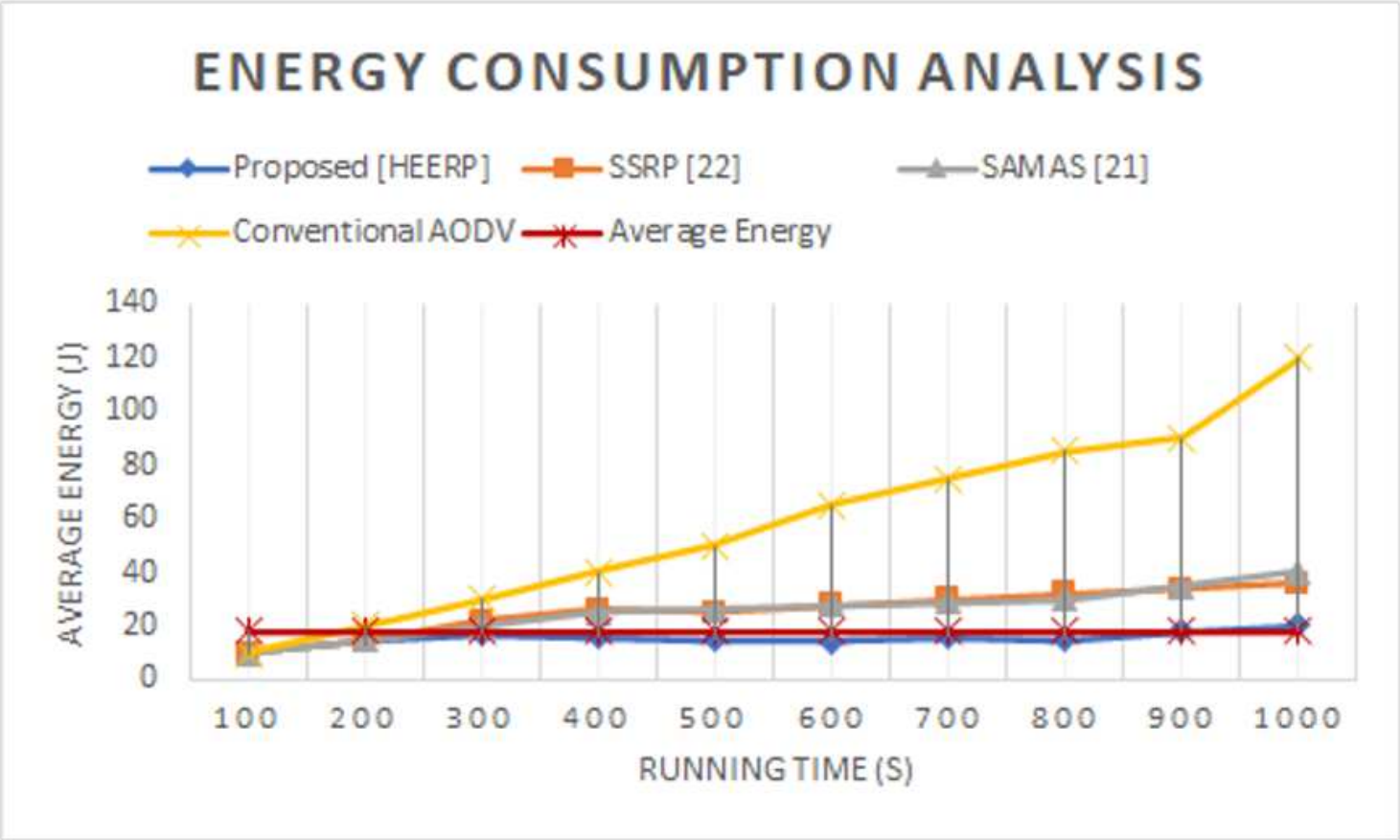

Figure 9

Energy Consumption Analysis