GENE POPULATED SPECTRAL CLUSTERING FOR ENERGY EFFICIENT MULTIPLE INTRUSION DETECTION AND RESPONSIVE MECHANISM FOR MANET

A.V.Santhosh Babu[1], Dr.P.Meenakshi Devi[2]

[1] Department of Information Technology
Sengunthar College of Engineering, Tiruchengode, Tamil Nadu-637205, India
santhoshbabu.av@gmail.com

[2] Department of Information Technology
K S R Institute for Engineering and Technology, Tiruchengode, Tamil Nadu-637215, India
drpmeenakshidevi@gmail.com

Abstract ─ A mobile ad hoc network (MANET) is a structure less network where the mobile devices are moved in random manner. In MANET, Each mobile device is randomly moves in various directions in the network. A few intrusions occurred due to the movement of mobile nodes in network. Mobile Nodes in an ad-hoc network are preserved by limited battery power for their operation. Hence, Energy management is a significant concern in a mobile ad-hoc network. In order to improve energy efficient multiple intrusion detection and responsive mechanism, Gene Populated Spectral Clustering (GPSC) technique is introduced in MANET. Initially, gene population generation is carried out to form a cluster. For each node, the energy and trust value is measured to detect the attacks. After that, various attacks such as grayhole, blackhole, wormhole, sleep deprivation and rushing attacks are identified through spectral clustering. The GPSC technique calculates the energy and trust value for each node in the cluster. Based on energy and trust value to select the cluster head and identify the intrusion levels. Finally, the intrusion response mechanism is performed from the intrusion level classifications. This helps to provide an efficient response with low network degradation. The severity of attack and the degradation in network performance provides efficient results from an implementation. Therefore, the proposed GPSC technique is more responsive to specific attack with spectral cluster. The simulation is carried out to analyze the performance of proposed GPSC technique with the parameters are energy consumption, intrusion detection rate and network lifetime.

Index Terms─ MANET, gene population generation, Spectral Clustering, energy, trust value, cluster head, intrusion detection, and responsive mechanism.

I. INTRODUCTION

MANET is a network in which the numbers of mobile nodes are connected without any access point. In MANET, the nodes perform communication within the transmission range. Due to free space, the various attackers from the MANET are presented. Therefore, protection of intrusion makes in the MANET is possible through the Intrusion Detection System.

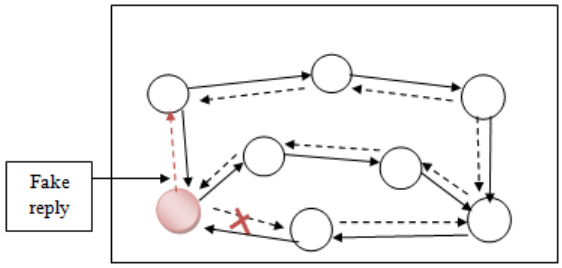

Figure 1 MANET with attack detection

Figure 1 shows the multiple mobile nodes contributes to perform efficient routing in MANET. In MANET, the numbers of mobile devices are deployed for communication within the transmission range. Most of the routing protocols perform efficient routing but the networks are more affected to various attacks. An intrusion detection system is introduced to monitor a network or systems for detecting the malicious activity violations. Therefore, it is clear that with lack of infrastructural support and vulnerable wireless link attacks, security is the intrinsic weakness in ad hoc network. In MANET, several intrusions are occurred to degrade the network performance and reduce the lifetime of the network. From that, the objective of the proposed work considers multiple network layer attacks

namely black hole, gray hole, sleep deprivation and rushing attacks. This type of attacks becomes more critical when a collection of malicious nodes combined with each other. Therefore, the detective and responsive mechanism presented against a various attack by multiple black hole nodes in a MANET. An efficient intrusion detection and adaptive responsive method is widely developed for MANETs that detects a variety of attacks and offers an effective response.

An intrusion detection and adaptive response mechanism (IDAR) was introduced in [1] to employ a grouping of both anomaly based intrusion detection and knowledge based intrusion detection techniques, and provides the MANETs against a variety of attacks. However, it failed to measure the node energy for enhancing the network lifetime.

In [2], Reliable Minimum Energy Cost Routing (RMECR) and Reliable Minimum Energy Routing (RMER) were introduced aiming at improving the energy efficiency and failed to perform the intrusion detection in MANET for efficient routing. In [3], an Enhanced Adaptive ACKnowledgment (EAACK) is an efficient intrusion-detection mechanism to protect MANET from attacks. However, the possibility of adopting the cryptography techniques improves the network overhead caused by digital signature. A secure and energy-efficient stochastic multipath routing protocol was introduced in [4] using Markov chain for MANETs. However, it is not only reduces chances of packet interception but also secures data transmission from route hijacking and jamming attacks.

Energy-efficient stable multipath routing was introduced in [5] measures the residual energy and links stability in the network. However, the battery level of the nodes is not efficient for enhancing the network lifetime. An Intelligent Energy-aware Efficient Routing protocol was designed in [6] for MANET (IE2R) but it provides heavy traffic conditions and to analyze the protocol.

In [7], statistical classification algorithms were designed to perform intrusion detection in MANETs. But it provided the classification error during malicious nodes and the various types of attacks detected. Binary Particle Swarm Optimization algorithm (BPSO) was designed in [8] to perform energy aware routing using TORA routing protocol for improving the network lifetime. An energy-conserving optimal path schedule algorithm was designed in [9] for improving packet delivery ratio with minimum energy consumption. However, the multiple attack detection remained unsolved to improve the secured routing in MANET. A proactive alleviation procedure was introduced in [10] for black hole attacks detection and responsive security method for identifying the malicious nodes in MANET. However, the other type's attacks were not addressed.

In this work, an efficient gene populated spectral clustering technique (GPSC) are introduced for energy efficient multiple intrusion detection in mobile ad-hoc network with the objective of addressing various attacks such as gray hole, black hole, wormhole, sleep deprivation and rushing attacks. The contributions of GPSC technique framework include the following:

To address energy efficient and multiple attack detection using a framework called, Gene Populated Spectral Clustering GPSC technique

To significantly perform the population generation based on energy and trust value using updated trust estimated value to widely detect the attacks in routing path

To improve intrusion detection rate, spectral clustering based on the condition estimated value of the nodes.

To reduce the energy consumption and improve network lifetime by applying responsive mechanism with spectral cluster to group the mobile nodes for routing in MANET.

The remaining part of the work is organized as follows: In Section 2, Gene populated spectral clustering (GPSC) technique is introduced in MANET with neat diagram. In Section 3 simulation settings is provided with detailed analysis of results explained in Section 4. In Section 5, introduce the background and review the related works. The conclusion of the research work is presented in section 6.

II. GENE POPULATED SPECTRAL CLUSTERING TECHNIQUE

One of the major challenges in the mobile network is resisting the several attacks. The various attacks cause a significant network traffic abnormality to affect the system performance for efficient routing. The several research works are not able to identify the multiple intrusion detection and responsive model patterns effectively. With this objective, a Gene Populated Spectral Clustering (GPSC) technique is introduced in the MANET. In GPSC technique, there are two different process are carried out such as, intrusion detection and responsive mechanism for handing multiple attacks in MANET. The GPSC technique detects a number of attacks and also significantly responds to the detected multiple attacks to reduce the damage caused by the attack and protect further attacks from the intruding nodes. Therefore, an intrusion response scheme offers the impact on network performance.

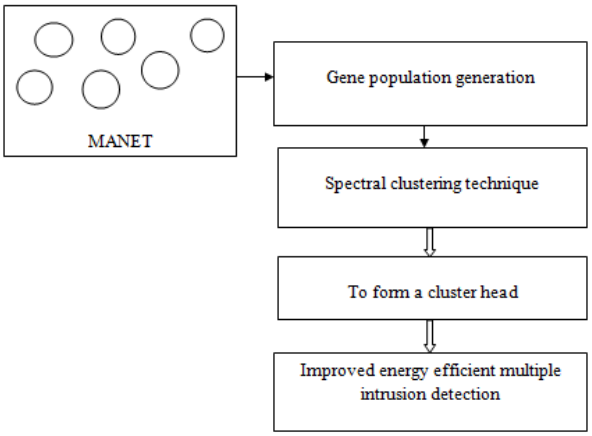

Figure 2 Flow processing diagram of the Gene Populated Spectral Clustering

Figure 2 processing diagram of the Gene Populated Spectral Clustering (GPSC) technique for improving energy efficient multiple intrusion detection and responsive technique. Initially, Gene population generation is performed to detect the intrusion in MANET. The trust value of the each node and their energy is calculated to transmit data packet to other nodes and it needs to discover a routing path and evaluate its trustworthiness. Hence it is used for measuring the reliability of each node on this path. After that, spectral clustering is carried out with different range of energy and trust value for cluster head selection. Based on these energy and trust value measurement, the proposed system is more responsive for calculates the confidence level of the attack that has been detected. The brief explanations about the different attacks are clearly illustrated as follows.

2.1 Gene population generation

Initially, the proposed (GPSC) technique starts from a population of randomly generated individuals and with these populations and the each iteration is called as generation. In each generation, the fitness of each individual in the population is calculated. In general, fitness is the objective function to provide the best solution. The number of individuals is selected from the population, to construct a new generation. This new generation is used for further processing. In MANET, numbers of nodes are considered as gene. Each member of this population initiates a feasible solution based on their fitness value. Initially, the population generation is carried out arbitrarily. After that, every iteration the best individuals (i.e. gens) are selected and the worst ones are restored with new ones generated from the fitness value. After generating the initial population, each individual is measured and assigned a fitness value along with the fitness function. The fitness value is measured based on the energy of the each gene and trust value.

Initially, all the mobile nodes contain initial energy for transmission. But during the transmission, energy level of nodes gets reduced. Therefore, the higher energy nodes are selected to form a cluster. These higher energy nodes are measured as follows,

$$\text{Energy (E)} = \text{Power (P)} * \text{time (T)} \qquad (1)$$

From (1), the energy (E) is measured with the product of the power and time. The unit of energy is in the joule (J), the unit of power is the watt (W), and the unit of time is the second (S). Based on energy measurement, higher energy nodes are selected for clustering. The energy used by mobile node for sending the n-bit of packet at the distance of 'D' meters is expressed as,

$$E_s = (E_U + E_{PA} * d) * n \qquad (2)$$

From (2), *Es* is the packet sending energy; E_U total energy utilization *d* represents the distance between the two nodes. Then, the energy of the node received the n-bit of packet is measured as,

$$E_R = E_U * n \qquad (3)$$

From (3), E_R energy of the node after receiving the n-bit of packet is multiplied with total energy E_U . Therefore, the nodes (genes) are selected based on their energy value to form a cluster.

Input: number of mobile nodes (i.e. gene)
'$MN_i = N_1, N_{2...} Nn$',
Output: measure the energy of node
Begin
Step 1 : Initialize the gene population
Step 2: for each mobile node
Step 3: Calculate the energy using (1)
Step 4: Measure energy used by mobile node for sending the n-bit of packet using (2)
Step 5: Measure energy used by mobile node for receiving the n-bit of packet using (3)
Step 6: obtain the higher energy nodes
Step 7 : End for
Step 8: end

Figure 3 energy measurement algorithms

As shown in the above algorithm, the gene population generation is carried out to measure the energy efficient node. At first, gene population is initialized randomly. For each iteration, the node energy is measured based on is the packet sending energy of node and after receiving the n-bit of packet energy. Therefore, highest energy nodes are selected to generate the population to form a cluster for identifying the intrusion in MANET.

2.1.1 Trust value based Node Authentication

After the computation of energy, the trust value of each node is determined. The trust value of the each node is measured based on the number of normal transmission service provided by nodes in MANETs. Therefore, trust value is defined as the difference between the numbers of data packets forwarded to the data packets dropped over the total number of data packets sent to neighboring mobile nodes. Therefore, trust is a value that measured based on nodes action when needed. Trust value of the nodes is measured to prevent node from various attacks like grayhole, blackhole, wormhole, sleep deprivation and rushing attacks.

In MANET, the sender transmits a RREQ messages to other neighbouring nodes and identifies the trusted node. The Route Reply (RREP) messages are sent from the neighboring node to source node. Therefore, the node has the highest trust value than the other nodes are selected for routing. Whenever, a source mobile node transmits data packets to the destination node, route request messages 'RREQ' are forwarded to the other neighboring nodes. Therefore, the route request transmitted from source node to neighbouring nodes is formulated as follows,

$$MN \rightarrow \sum_{i=1}^{n} RREQ\ (NN_i) \qquad (4)$$

From (4), mobile node *(MN)* transmits the route request *RREQ* to the neighboring node NN_i the neighboring node sent reply message,

$$NN \rightarrow RREP\ (MN) \qquad (5)$$

Based on the Route Reply (RREP) messages and request messages 'RREQ', the trust value of node is identified. Based on the RREQ and RREP packet transmission, the trust value is measured only the data packet dropped and number of data packet received at destination and total number of packet sent from source node.

$$trust\ value_{MN} = packet_{s/}\ packer_{s} \qquad (6)$$

From (6), trust value of mobile node ($trust\ value_{MN}$)is identified based on the number of packet sent from source node and received by destination based on route request and reply message. Then the threshold values are assigned to measure the trust value of node. If the trust value of the node is higher than the threshold value, then the node is said to be a trusted node to perform transmission otherwise the node is unsecured. In order to measure the trust value of node, the source node has to monitor the following factors,

Table 1 trust table

Node ID	packet sent (SN)	packet received (DN)	packet dropped	Trust value

Hence, the data packets sent is measured as the percentages of data packets initiated from the mobile node MN_i that is transmitted over the total number of data packets distributed. The number of data packets dropped over the total number of data packets sent. Hence, the data packets dropped is expressed as follows,

$$DPD = \frac{\text{number of data packets dropped}}{DP_i} \qquad (7)$$

From (7), where *DPD* is the data packet dropped and DP_i is data packet sent from source node (SN). Therefore, the higher trust values of mobile nodes are selected for routing in order to avoid the attacks.

// Trust value based Node Authentication
Input: Mobile Nodes '$MN_i = MN_1, MN_2, \dots, MN_n$' Source Node '$SN$', Destination Node '$DN$', , Data Packets '$DP_i = DP_1, DP_2, \dots, DP_n$'
Output: calculate the trust value of node
Step 1: Begin
Step 2: **For** each Mobile Node 'MN_i'
Step 3: Measure Data Packet Drop Rate using (7)
Step 6: Evaluate trust factor of (6)
Step 7: **If** ($Trust\ factor_{MN_i} > threshold$)
Step 8: Node is secured and Perform data packet transmission
Step 9: **Else**
Step 10: Node is unsecured failed transmission
Step 11: **End if**
Step 12: **End for**
Step 13: End

Figure 4 Trust value based Node Authentication

As shown in figure 4, the trust value of the node is identified based on the number of packet sent, received and packet dropping capability of the nodes. Therefore, GPSC technique estimates the trust value for all the mobile nodes thereby it authenticates neighbouring nodes to form cluster for secured data transmission in MANETs. Therefore, the packet delivery and secure transmission is achieved in a significant manner.

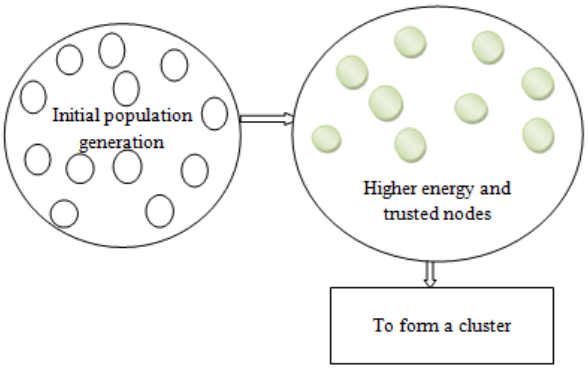

Figure 5 Initial population generation

Figure 5 shows factors that influence the initial population is generated randomly based on their energy and trusted nodes in the network. From the figure, gene population generation is carried out and it indicates green color.

2.2 Spectral clustering for intrusion detection and responsive mechanism

Once the population of gene is generated based on the energy and trust value of the node then the clustering is formed using spectral clustering technique. And the cluster head is selected for identifying the intrusion in MANET. In GPSC, the cluster is formed based on the energy and trust value of the nodes. The node which has higher energy and trust value is selected as cluster head for specific intrusion detection in MANET.

2.2.1 Spectral clustering

The spectral clustering is used in GPSC technique to increase an alert for a possibility of several attacks and to extract attack for future information distribution. A spectral clustering technique utilizes the spectrum of the similarity pair of the node for reducing the dimensionality. A spectrum is a state that not restricted to a specific set of values but it differs without steps across a range. The similarity of node is provided as an input and it performs quantitative evaluation of the relative pair of nodes in the network. The relative pair of the nodes is identified through the trust and energy value of the nodes in MANET. The proposed gene populated clustering method classifying attacks and of distinguish the types of attacks.

Let us consider the number of mobile nodes in the MANET, MN_i and the similarity between the nodes are measured using the weight matrix,

$$w_{ij} = f\left(\left\|MN_i, MN_j\right\|, \sigma\right) \quad (8)$$

From (8),W_{ij} is the weight matrix between the similarity function of two mobile nodes and σ is the scaling parameter. The scaling parameter is used to find the local structure of the connections between nodes in Network. Each node has the various two weighting factor such as Energy (E) and trust value (TV). Based on the weighting factor, the cluster head identifies what types of attacks present in the routing path. The node which has higher trust value is a normal one and the security level is extremely high. The node which has lower trust value represent the attack or malicious node presented in the network. Therefore, the diagonal matrix 'D' is defined through the weight matrix,

$$d_{ij} = \sum_{i,j=1}^{n} w_{ij} \quad (9)$$

Therefore, the spectral clustering is a dominant tool for clustering the nodes based on similarity function and the scaling parameter. Based on the trust value of the node the intrusion is detected and it classified as different condition. The similarity between the two nodes are depends on the both energy and trust value.

$$Low\ energy + High\ trust = LE + HT \quad (10)$$

$$Low\ energy + Low\ trust = LE + LT \quad (11)$$

$$Low\ trust + High\ energy = LT + HE \quad (12)$$

$$High\ energy + High\ trust = HE + HT \quad (13)$$

Based on above said four types of trust value and energy pair, the cluster are formed where every node belongs to at least one cluster. The nodes in every cluster choose a cluster head to identify the intrusion in network.

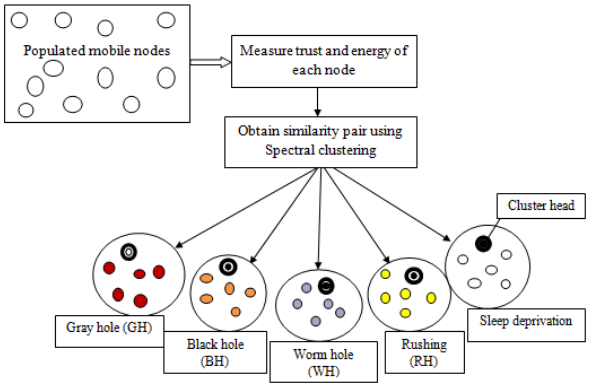

Figure 6 spectral clustering for multiple intrusion detection

Figure 6 illustrates the spectral clustering is described for identifying the multiple intrusion detection. From the figure, the numbers of populated genes are randomly deployed. Then the energy and trust value of the each node is measured for efficient routing. Based on the energy and trust value, the relative pair of the nodes is obtained using spectral clustering. Through the populated nodes, the similarity pair of the nodes is clustered to identify the particular attacks in MANET. Spectral clustering is the most significant technique for the energy saving and multiple intrusion detection. This

type of routing reduces the network traffic and improves the reliability of the network through the CHs to remove redundant data in MANETs. Therefore, it reduces the overall energy consumption of the network by transmitting the aggregated data.

2.2.2 Responsive mechanism

Gray hole attack: Initially, the clustered red colored nodes are deployed in network to identify gray hole attacks though the condition of low energy and higher trust value *(LE + HT).* These pair of the nodes is deployed in the mobile network to identify the gray hole attacks. These types of attack are a kind of selective forwarding attack and the malicious nodes attempts to drop the data packets in transmission. This attack drops all packets during the transmission. Therefore, this attack reduces the network lifetime. In order to detect such kind of attacks, GPSC technique uses the spectral clustering to find the energy and trust value. It first checks the node id and address in order to avoid node duplication. If the trusted node is already listed either permanently or temporarily then the node prevents unnecessary network traffic. Otherwise, the node checks the response from trusted node.

Black hole attack: The second type of attack is the black hole attack to drop the data packets. It occurs during the transmission of the data packets. If, a malicious node is presented in the network that does not maintains RREQ packet and RREP packets between the nodes. The node receives the RREQ packet; it sends a false RREP packet to the source node directly within a network. This attack in the networks is identified using spectral clustering technique with the condition of low energy with low trust value. From the figure 4, a node with orange color indicates the low energy with low trust value for identifying the black hole attack effectively and the cluster head selects the trusted node, and isolates the attacks from the network. After that, it immediately ignore all packets in the queue.

Wormhole attack: The third type of attack is a wormhole attack. In MANET, an attacker attains packets from the one end in the network which is called as "tunnels" to other end in the network. This tunnel among the two attacks is called as a wormhole. Wormholes are difficult to identify path that is not used to transfer the information in the network. Wormholes attacks are unsafe since they damage the network. Therefore, these types of the attacks are detected using GPSC technique. The proposed spectral clustering is used for grouping the nodes with lower trust value and higher energy *(LT + HE).* These types of nodes are colored in violet. Therefore, the cluster head are deployed in network to identify the wormhole attack and isolate the attacks effectively.

Rushing attack: The Rushing attack is other types of intrusion which degrades the network performance. When a source node forwards a route request packet to other node in the network. If there is an attacker occurred, then the other accepts the request packet and sends to his neighboring node with high transmission. Due to high transmission speed, packet transmitted by a attacker is first arrive at the destination node. Destination node accept this RR packet and reject other packets which are arrived later. Therefore, the destination node determined as a valid route and use for further communication in GPSC technique. This way attacker effectively distracts the communication between nodes. Therefore, the proposed gene populated spectral clustering approach improves the packet transmission where the node has the condition of high energy and high trust value *(HE + HT).*(Based on this condition, the group of yellow colored nodes is deployed in network to effectively detect and isolate the rushing attacks.

Sleep deprivation: In this scenario, the intrusion response scheme with a Sleep deprivation (SD) attack is presented. SD is a severe DoS attack that frequently causes significant damage to the mobile network. In sleep deprivation attack, the attacker utilizes the route discovery process through RREQ and RREP control packets in order to informs each node constantly and consume its restricted resource of energy, bandwidth, and memory. In figure 4, the remaining node other than the colored node is deployed to identify the Sleep deprivation attacks. In GPSC technique, the RREQ and RREP control packets are transmitted for measuring the trust value of the node and separates the attacks present in the network.

Therefore, the proposed GPSC technique is used to cluster the trusted node and to isolate the intrusion from the network. The proposed method is more responsive to specific attacks with spectral clustering technique.

III. SIMULATION SETTINGS

An efficient a Gene Populated Spectral Clustering (GPSC) technique is implemented in NS2.34 network simulator. Totally 500 nodes are deployed within the network range of 1500 m*1500 m size. The Ad hoc on demand distance vector routing protocols (AODV) is used to analyze the performance of the proposed intrusion identification and response system. The propagation range for every mobile node in the network is around 250 meters. The Channel capacity is fixed as 2 M bits/sec. A constant bit rate is used as type of traffic to perform simulation. The nodes' mean speed varies from 0 to 20 m/s. The node mobility uses the random waypoint model. In the following tests, different types of routing attacks, i.e., black hole (BH), grayhole (GH), wormhole (WH), sleep deprivation (SD) and rushing attacks (RH) are detected. The simulation parameter is shown in following table 2.

Table 2 Simulation Parameters

Simulation parameter	Value
Simulator	NS2 .34
Protocol	AODV
Number of nodes	50,100,150,200,250,300,350,400,450,500
Simulation time	2000sec
Mobility model	Random Way Point
Nodes speed	0-20m/s
Network area	1500m * 1500m
Data packets	10,20,30,40,50,60,70,80,90,100
Number of runs	10
Traffic type	CBR

IV. RESULT ANALYSIS

The result analysis of GPSC technique is performed and compared with two existing methods namely intrusion detection and adaptive response mechanism (IDAR) [1] reliable minimum energy cost routing (RMECR) mechanism [2]. In order to evaluate the performance of GPSC technique, a network consisting of 500 nodes within the area and uses Random Waypoint Model as the mobility model. The various simulation parameters such as energy consumption, intrusion detection rate and network lifetime are explained with the help of tables and graphs.

4.1 Impact of energy consumption

Energy consumption is measured using the amount of energy consumed by a single mobile node with respect to the total mobile nodes in MANET. The energy consumption is mathematically formulated as given below.

$$EC = Energy_{SN} * TotalMN \quad (14)$$

From (14), the energy consumption '*EC*' on transmission is obtained by the product of the energy for single node '$Energy_{SN}$' and total mobile nodes '$Total_{MN}$' in the network. The energy consumption is measured in terms of Joules. Minimum energy utilization is obtained to improve the network lifetime.

Table 3 Tabulation for Energy consumption

No. of nodes	Energy consumption (joules)														
	BH attack			GH attack			WH attack			RH attack			SD attack		
	GPSC	IDAR	RMECR	GPSC	IDAR	RMECR	GPSC	IDAR	RMECR	GPSC	IDAR	RMECR	GPSC	IDAR	RMECR
50	25	49	40	28	52	43	31	53	44	35	55	46	38	58	48
100	27	53	44	32	55	47	34	57	48	38	59	50	40	62	51
150	31	55	46	35	57	48	38	60	50	42	62	51	43	65	53
200	33	60	50	38	61	51	43	63	53	46	65	54	48	68	56
250	35	62	54	42	63	55	46	65	57	50	68	58	52	70	60
300	38	67	59	44	70	61	53	71	62	55	72	63	57	73	65
350	43	71	65	47	73	66	55	75	67	58	76	68	60	78	70
400	51	80	74	55	81	75	63	83	77	65	85	78	67	86	79
450	63	85	79	67	86	80	69	87	82	70	88	83	73	90	84
500	74	96	87	78	97	89	80	99	90	82	106	92	84	112	95

Table 3 describes energy consumption with the presence of the five different types of attacks over the network. The energy of the each node is measured based on the power and time. Therefore, the total energy consumed by the node is measured in proposed GPSC technique and existing (IDAR) [1] and Reliable minimum energy cost routing (RMECR) [2] mechanism. The performance analysis of the methods is illustrated in figure 7.

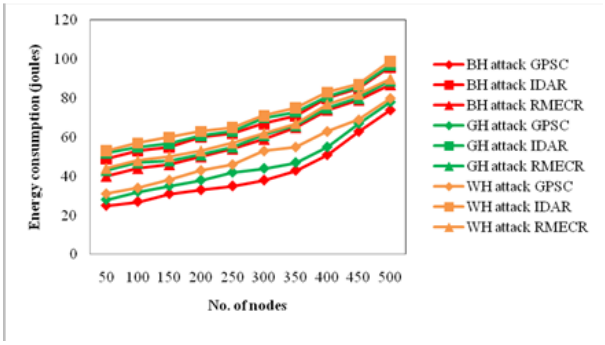

Figure 7 (a) Measure of energy consumption

Figure 7 (a) shows the energy consumption during transmission based on the number of node in MANET considered for experimental purposes. The proposed GPSC technique performs relatively well when compared to two existing methods. The energy consumption on transmission is reduced in the GPSC technique by applying gene populated spectral clustering technique. The impact of response action on energy consumption in network with the presence of BH, GH, WH, RH and SD attacks. This provides efficient result in minimizing the energy consumption. Let us consider with the presence of the black hole attack, the energy consumption of the proposed GPSC technique gets reduced. In GPSC technique, the higher energy and trust nodes are selected for routing process. Based on energy utilized by mobile node for sending the n-bit of packet and energy of the node received the n-bit of packet. Therefore, highest energy nodes are selected to generate the population in MANET. This helps to reduce the energy consumption. Therefore, the energy consumption is reduced by 40% and 31% compared to existing IDAR [1] and RMECR [2] mechanism respectively.

With the presence of gray hole attack over the network during the data packet transmission, the higher energy nodes are selected for transmission. Gene population generation is performed in the design of GPSC technique to initiate a possible. Therefore, the energy utilization of the GPSC technique is reduced by 34 % and 25% then the existing methods. In addition, the energy consumption with the presence of the worm hole attack is reduced using GPSC technique. The GPSC technique utilizes the minimum amount of energy for detecting the attack in environments. Therefore, amount of energy consumed by 30% and

20% when compared to existing IDAR [1] and RMECR [2] respectively.

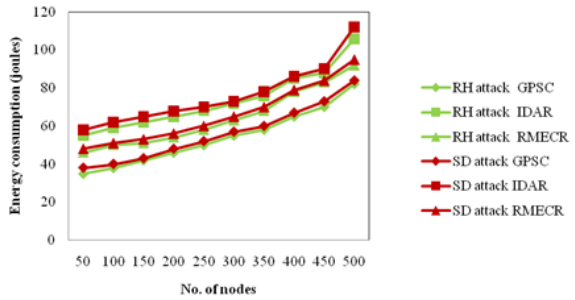

Figure 7(b) Measure of energy consumption for RH and SD attacks

Figure 7(b) illustrates the impact of response achievement on energy consumption in network with the presence of RH attacks and SD attacks. This result shows the proposed GPSC technique minimizes energy consumption while increasing the number of nodes in the network. A spectral clustering technique is applied for grouping the energy efficient and trust based nodes to transmit the data packet between the nodes. From that, the total best path is selected for energy efficient routing, without any intrusion. Therefore, this helps to reduce the energy consumption thereby improving the network lifetime. The energy consumption during the data packet transmission gets reduced by 27% and 16% with the presence of rushing attack over the network compared to existing IDAR [1] and RMECR [2]. In addition, with the occurrence Sleep deviation attack in the network, the proposed gene populated spectral clustering technique performs the relative pair of energy and trust measurement. As a result, the utilization of the energy is considerably reduced by 30% and 16% than the existing IDAR [1] and RMECR [2] respectively.

4.2 Impact of intrusion detection rate

Intrusion detection rate is defined as the ratio of the number of normal nodes and the number of malicious nodes to the total number of nodes in the network. The formula for intrusion detection is expressed as follows,

$$IDR = \frac{Number\ of\ normal\ nodes - No.of\ malicious\ nodes}{Total\ No.of\ nodes} * 100 \quad (15)$$

From (15), IDR is the intrusion detection rate which is measured in terms of percentage (%). Higher the intrusion detection rate more efficient the method is said to be.

Table 4 Tabulation for Intrusion detection rate

No. of nodes	Intrusion detection rate (%)														
	BH attack			GH attack			WH attack			SD attack			RH attack		
	GPSC	IDAR	RMECR	GPSC	IDAR	RMECR	GPSC	IDAR	RMECR	GPSC	IDAR	RMECR	GPSC	IDAR	RMECR
50	80	68	56	78	66	55	77	65	54	75	63	53	72	61	51
100	82	70	58	80	68	56	79	67	55	77	65	54	74	63	52
150	84	72	60	82	69	58	80	68	56	79	67	55	76	65	53
200	86	75	62	84	72	60	82	70	59	80	69	57	78	68	55
250	88	78	64	86	75	62	84	72	61	82	71	59	80	70	57
300	90	80	68	88	77	65	86	74	62	84	73	60	82	72	59
350	92	82	70	90	78	68	88	76	65	86	75	63	84	73	61
400	94	84	72	92	79	70	90	78	68	88	76	67	86	75	64
450	95	86	74	94	82	72	91	80	70	89	78	68	88	76	67
500	96	90	76	95	86	74	93	82	72	91	81	70	90	79	69

As shown in table 4, the analysis of intrusion detection rate based on the number of node ranges from 50 to 500. The targeting results of five types of attack using (IDAR) [1] reliable minimum energy cost routing (RMECR) mechanism [2] are shown in following figure.

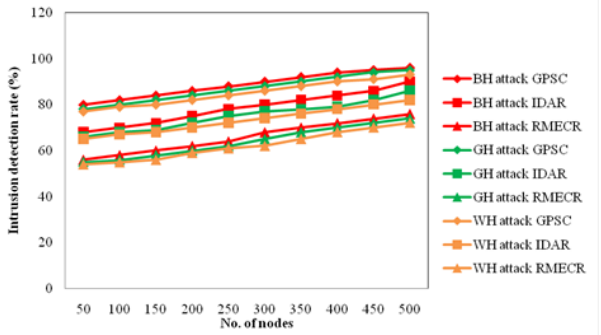

Figure 8 (a) Measure of intrusion detection rate for BH, GH and WH attacks

Figure 8 (a) shows the intrusion detection rate with respect to number of mobile nodes in network. While varying the number of nodes, the intrusion detection rate gets increased in all the methods with different attacks. From the figure, the red color indicates the black hole attacks whereas green color curve indicates gray hole attacks and orange color line denotes wormhole attacks. Therefore, three different types of attacks are clearly described as shown in figure. Let us consider black hole attack, the intrusion detection rate with proposed GPSC technique is compared with existing methods. From that, the proposed GPSC technique improves the intrusion detection rate than the existing approaches. This improvement is obtained due to the application of spectral clustering technique. Initially, Gene population generation is carried out based on the energy and trust value in order to form the cluster. For improving the intrusion detection rate, the trust value of each node in the population generation and their energy is measured to form a cluster head. The higher trust value of the node is identified to transmit data packet through the selected nodes. This

helps for avoiding the intrusion in network. In addition, the spectral clustering is used to cluster the populated nodes with the condition of low energy with low trust value. Therefore, the nodes which has these condition is selected and it is more responsive for blackhole attack in MANET. As a result, the proposed GPSC technique considerably increases the intrusion detection rate by 13% and 35% as compared to existing IDAR [1] RMECR mechanism [2] respectively with the presence of black hole attack.

The intrusion detection rate is increased in proposed GPSC technique with the presence of the gray hole attack in MANET than the existing methods. This type of attack is a selective forwarding attack. During the data packet transmission, the malicious nodes through this attack challenges to drop the data packets. This helps for reducing the packet transmission between source and destination. Such kind of attacks is reduced by using GPSC technique due to condition of low energy and high trust value. The proposed Spectral clustering groups the nodes to identify the gray hole attack in MANET. Therefore, the intrusion detection rate is increased by 16% and 36% using GPSC technique than the existing IDAR [1] RMECR [2] mechanism respectively.

Let us considering the data packet transmission between the source node and destination with the presence of worm hole attack in MANET. An attacker presence in the network from one end to other end is called as "tunnels". This tunnel is called as wormhole. Therefore, the populated spectral clustering is applied for grouping the populated nodes with the condition of lower trust value and higher energy. The spectral clustering is used to find the similarity of node and it provides relative pair of nodes in the network. The qualified pair of the nodes is obtained through trust and energy value of the each populated nodes in MANET. Therefore, the proposed GPSC technique increases the intrusion detection rate by 16% and 37% than the existing methods [1][2] respectively.

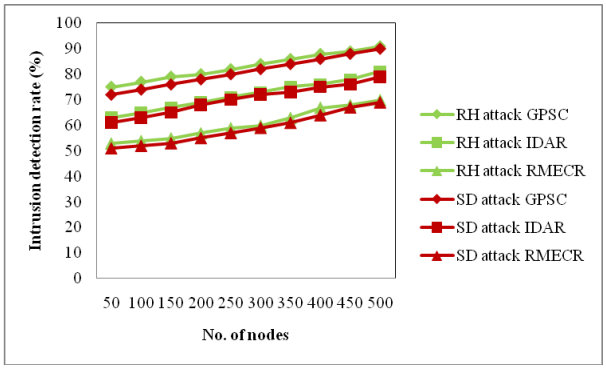

Figure 8 (b) Measure of intrusion detection rate for SD attack and RH attack

Figure 8 (b) illustrates the intrusion detection rate for SD attack and RH attack with number of mobile nodes deployed in the mobile network. From the figure, it is clearly evident that while varying the number of nodes, the intrusion detection rate gets increased in proposed GPSC technique due to the different energy and trust value condition measurement. From the figure intrusion detection is identified with two attacks such as SD attacks and RH attacks. The green color curve indicates intrusion detection with SD attacks and the brown color line indicates intrusion detection with RH attacks.

The proposed GPSC technique improves the intrusion detection rate with the presence of RH attacks. The Rushing attack is types of intrusion which reduces the network performance. When a source node forwards a data packet, the distention not receives any packet due to attack presence in the network. Therefore, the proposed gene populated spectral clustering approach improves the transmission where the populated nodes have high energy and high trust value ($HE + HT$). With the higher energy and trust value of the node is selected for avoiding the packet drops and effectively detects the rushing attacks. The GPSC technique improves the intrusion detection rate by 16% and 38% compared to existing IDAR [1] RMECR [2] mechanism respectively. Finally, the sleep deprivation attacks are identified over the MANET using GPSC technique. With the presence sleep deprivation attack in MANET, the abnormal rate of the energy and trust value indicates the sleep deprivation attack. Therefore, this kind of attacks is identified using multiple intrusion detection GPSC technique. The intrusion detection rate is significantly improved by 15% and 38% than the existing IDAR [1] RMECR [2] respectively.

4.3 Impact of network lifetime

Network life time is defined as the ratio of number of higher energy nodes is selected for performing energy efficient routing to the total number of nodes deployed in network. It is measured in terms of percentage (%). The formula for network lifetime is given below,

$$NL = \frac{No.of\ HE\ nodes}{No.of\ nodes} * 100 \quad (16)$$

From (16), Where NL is the network lifetime and $No.of\ Higher\ Energy\ (HE)\ nodes$ is selected for efficient routing in MANET

Table 4 Tabulation for network lifetime

No. of nodes	Network lifetime (%)														
	BH attack			GH attack			WH attack			RH attack			SD attack		
	GPSC	IDAR	RMECR	GPSC	IDAR	RMECR	GPSC	IDAR	RMECR	GPSC	IDAR	RMECR	GPSC	IDAR	RMECR
50	84	69	78	82	67	77	81	65	75	80	63	74	79	60	73
100	85	72	79	83	70	78	82	68	76	81	67	75	80	65	74
150	86	74	80	84	73	79	83	70	78	82	69	77	81	67	75
200	87	75	81	85	74	80	84	72	79	83	70	78	82	69	76
250	89	76	82	86	75	81	85	74	80	84	72	79	83	70	78
300	90	77	83	87	76	82	86	75	81	85	74	80	84	72	79
350	92	78	84	89	77	83	87	76	82	86	75	81	85	74	80
400	94	80	85	91	79	84	89	77	83	87	76	82	86	75	81
450	95	81	86	92	80	85	90	78	84	88	77	83	87	76	82
500	96	83	89	94	82	87	93	80	86	92	79	85	91	78	84

Table 4 describes the targeting results of network lifetime measurement based on the number of mobile nodes in the network. The numbers of nodes in the network is deployed in the network for secured transmission and avoid the multiple intrusions in MANET. Therefore, the proposed GPSC technique improves the network lifetime than the existing IDAR [1] RMECR [2]. The figure 7 (a) and (b) shows the simulation result of the network lifetime with five different types of attacks over the network.

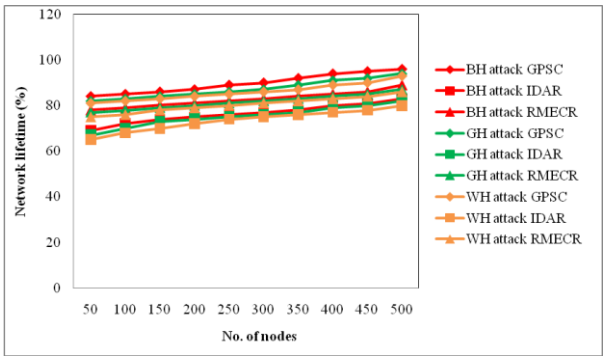

Figure 9 (a) Measure of network lifetime for presence of BH, GH and WH attacks

Figure 9 (a) depicts the performance result of the network lifetime with the number of nodes deployed in mobile network. The network life time is improved based on minimum energy consumption and detect the multiple intrusion in MANET. In MANET, each populated nodes has higher transmission power and it consumes minimum energy for transferring the data packet through the network. The GPSC technique improves the network performance with the minimum energy consumption and higher trust value than the existing methods. The energy of the each node is measured for performing the efficient transmission. The node weighting function is measured based on the higher energy and trust value between the nodes. From that, the node which has best value is selected for routing. In GPSC technique, each mobile node has high power which helps to extend the network lifetime. From the figure, the network lifetime with the presence of the three different attacks BH, GH and WH are described and it indicates three different colors. Therefore, the network lifetime is increased using GPSC technique by 17% compared to existing IDAR [1] RMECR [2] with the presence of black hole attacks. In addition, the proposed GPSC technique improves the network lifetime with the presence of the gray hole attack. Therefore, the network lifetime is increased by 16% and 7% compared to existing methods. Finally, the network lifetime is improved by 17% and 7% using proposed gene populated spectral clustering technique compare to IDAR [1] RMECR [2] with the presence of wormhole attack .

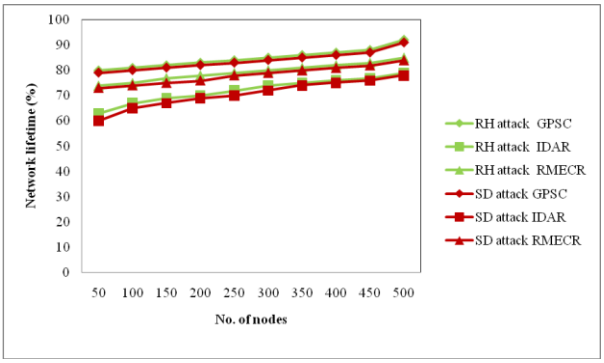

Figure 9(b) Measure of network lifetime for presence of RH attack and SD attack

Figure 9(b) analyses the network life time imposed on the MANETs based on the number of nodes in network. In order to enhance the network life, the attacks present in the current path is identified and it is affects the intrusion node. In order to varying the number of mobile nodes from 50 to 500 in networks and the network life time is analyzed by performing the various response action route around the attacks and isolation with BH, GH, WH, SD and RH attacks. The result shows the proposed GPSC technique maximizes the network life time and it is more vulnerable against the attacks in ad hoc network. In MANET, several intrusions are presence to degrade the performance of the network thereby reducing the lifetime of the network. The objective of the GPSC technique performs energy measurement and trust value for grouping the nodes to detect multiple network layer attacks. Therefore, the network lifetime is considerably increased in proposed GPSC technique by 18% and 7% with the presence of Rushing attack (RH). Moreover, the overall network lifetime is increased by 19% and 7% using GPSC technique than the existing IDAR [1] RMECR [2] with the presence of sleep deprivation.

As a result, the analysis of the proposed Gene Populated Spectral Clustering (GPSC) technique shows the significant improvement in energy consumption, intrusion detection rate and network lifetime with the presence of multiple attacks over the network.

V. RELATED WORKS

In MANET, the source transmits a data packet to a target node depends on energy efficient and intrusion detection. Therefore, the various routing techniques were introduced to shows the proposed technique performance.

A dynamic fuzzy energy state based AODV (DFES-AODV) routing protocol was introduced in [11] for Mobile Ad-hoc NETworks (MANETs). However, it still needs experimental adjustment of a number of functional parameters. This problem is overcome by proposed GPSC technique with different performance parameter.

A distributed packet dropping attack (PDA) detection technique named NAODV was developed in [12] for Detecting and isolating the malicious node presented in transmission depends on measurement of trust level of the nodes. But it failed to consider the multiple attacks and battery power utilization. This problem is addressed by using gene populated spectral clustering for satisfying the specific conditions.

A Detection and Isolation Packet Dropped Attackers in MANETs (DIPDAM) was described in [13]. However, it failed to detect both data packet attackers and route packets attackers. The proposed GPSC technique detects multiple attacks and provides the effective response in MANET.

In [14], A Gray hole attack was detected in mobile ad hoc networks and to identify the malicious node. But, it takes more time for detecting attack in network. The proposed spectral clustering technique is used to identify the attack with minimum time.

A risk-aware response mechanism was introduced in [15] to analytically handle the routing attacks in MANET. However, the performance and utility of the method was not extended. The performance of the intrusion detection technique is extended by proposed GPSC technique with different parameter.

A Vickrey–Clarke–Groves mechanism was introduced in [16] for cluster leader selection process which improves the intrusion detection service. But, the intrusion detection rate was not improved effectively. In GPSC technique, the higher intrusion detection rate is obtained with presence of multiple attacks.

A data transmission quality function (DTQ) was developed in [17] for identifying the behavior of the malicious node in MANET. However it failed to detect the various types of attacks in MANET. This problem is overcome by using GPSC based multiple intrusion detection system.

Conformal Prediction K-Nearest Neighbor algorithmic rule was designed in [18] for classifying the attack. But, a broad variety of circumstances including various attack types were not addressed. The GPSC technique is more responsive to avoid the particular attack in MANET.

An Energy-Aware Span Routing Protocol was designed in [19] that utilize the energy-saving approaches to improve the network lifetime. The GPSC technique uses the minim energy consumption for routing thereby improving the network lifetime. A clustering technique in Ad-hoc On-demand Distance Vector (AODV) routing protocol was designed in [20] for detecting and preventing the black-hole attack in MANETs. But, it failed to provide the effective result through the performance analysis. The proposed GPSC technique improves the efficient performance results in terms of energy consumption, intrusion detection and network lifetime.

VI. CONCLUSION

An efficient Gene Populated Spectral Clustering (GPSC) technique is developed for energy efficient multiple intrusion detection in MANET. In GPSC technique, two phase enhanced intrusion detection and response mechanism for multi hop routing for MANETs. Initially, the gene population generation is carried out based on calculation of energy and trust value. After that, various attacks are identified through spectral clustering and to calculate the trust value and energy for each node in the cluster. Based on the energy and trust value to select the cluster head and detects the intrusion levels. Finally the intrusion responsive mechanism is performed for classifying the intrusion based on the different condition evaluation through the spectral clustering. The proposed spectral clustering technique provides more responsive to a specific attack in MANET. The simulation is carried out for different parameters such as energy consumption, intrusion detection rate and network lifetime. The performance results show that the GPSC technique improves the intrusion detection rate, network life time and reduces the energy consumption than the state-of-art methods.

REFERENCES

[1] Adnan Nadeem and Michael P. Howarth, “An intrusion detection & adaptive response mechanism for MANETs”, Ad Hoc Networks, Elsevier, Volume 13, 2014, Pages 368–380

[2] Javad Vazifehdan, R. Venkatesha Prasad, and Ignas Niemegeers," Energy-Efficient Reliable Routing Considering Residual Energy in Wireless Ad Hoc Networks", IEEE Transactions on Mobile Computing, Volume 13, Issue 2, 2014, Pages 434 – 447

[3] Elhadi M. Shakshuki, Nan Kang, and Tarek R. Sheltami, "EAACK—A Secure Intrusion-Detection System for MANETs", IEEE Transactions on Industrial Electronics, Volume 60, Issue 3, 2013, Pages 1089-1098

[4] Sajal Sarkara and Raja Datta, "A secure and energy-efficient stochastic multipath routing for self-organized mobile ad hoc networks", Ad Hoc Networks, Elsevier, Volume 37, 2016, Pages 209–227

[5] A. Pratapa Reddy and N. Satyanarayana, "Energy-efficient stable multipath routing in MANET", Wireless Networks, Springer, 2016, Pages 1–9

[6] Santosh Kumar Das and Sachin Tripathi, "Intelligent energy-aware efficient routing for MANET", Wireless Networks, Springer, 2016, Pages 1–21

[7] Aikaterini Mitrokotsa , Christos Dimitrakakis , "Intrusion detection in MANET using classification algorithms: The effects of cost and model selection", Ad Hoc Networks, Elsevier, Volume 11, 2013, Pages 226–237

[8] Shahram Jamali, Leila Rezaei, Sajjad Jahanbakhsh Gudakahri, "An Energy-efficient Routing Protocol for MANETs: a Particle Swarm Optimization Approach", Journal of Applied Research and Technology, Volume 11, Issue 6, December 2013, Pages 803–812

[9] Young-jun Oh and Kang-whan Lee, "Energy-efficient and reliable routing protocol for dynamic-property-based clustering mobile ad hoc networks", International Journal of Distributed Sensor Networks, Volume 13, Issue 1, 2017, Pages 1-16

[10] M. Rajesh Babu S. Moses Dian, Siva Chelladurai and Mathiyalagan Palaniappan, "Proactive Alleviation Procedure to Handle Black Hole Attack and Its Version", Hindawi Publishing Corporation, The Scientific World Journal, Volume 2015, August 2015, Pages 1-12.

[11] Saloua Chettibi and Salim Chikhi, "Dynamic fuzzy logic and reinforcement learning for adaptive energy efficient routing in mobile ad-hoc networks", Applied Soft Computing, Elsevier, Volume 38, 2016, Pages 321–328

[12] Bobby Sharma Kakoty, S. M. Hazarika and N. Sarma, "NAODV- Distributed Packet Dropping Attack Detection in MANETs, "International Journal of Computer Applications, Volume 83, Issue 11, 2013, Pages 29-35

[13] Ahmed Mohamed Abdalla, Ahmad H. Almazeed, Imane Aly Saroit and Amira Kotb, "Detection and Isolation of Packet Dropping Attacker in MANETs", International Journal of Advanced Computer Science and Applications (IJACSA),Volume 4, Issue 4, 2013, Pages 29-34

[14] Ashok M. Kanthe, Dina Simunic, Ramjee Prasad," A Mechanism for Gray Hole Attack Detection in Mobile Ad–hoc Networks", International Journal of Computer Applications Volume 53, Issue 16, 2012, Pages 23-30

[15] Sk.Rahima Sulthana, D.Srujan Chandra Reddy, T.Bharath Manohar, "An Efficient Mechanism of Handling MANET Routing Attacks using Risk Aware Mitigation with Distributed Node Control", International Journal of Modern Engineering Research (IJMER), Volume 3, Issue 5, 2013, Pages 2996-3004

[16] Basant Subba, Santosh Biswas and Sushanta Karmakar, "Intrusion detection in Mobile Ad-hoc Networks: Bayesian game formulation", Engineering Science and Technology, an International Journal, Elsevier, Volume 19, Issue 2, 2016, Pages 782–799

[17] S.Mamatha and A. Damodaram, "Intrusion Detection System for Mobile Ad hoc Networks Based on the Behavior of Nodes", International Journal of Grid Distribution Computing, Volume 7, Issue 6, 2014, Pages 241-256

[18] M. Lalli and V. Palanisamy, "A Novel Intrusion Detection Model for Mobile Ad-hoc Networks using CP-KNN", International Journal of Computer Networks & Communications (IJCNC), Volume 6, Issue 5, 2014, Pages 193-201

[19] G. Ravi and K.R. Kashwan, "A new routing protocol for energy efficient mobile applications for ad hoc networks", Computers & Electrical Engineering, Elsevier, Volume 48, 2015, Pages 77–85

[20] Rashmi, Ameeta Seehra," A Novel Approach for Preventing Black-Hole Attack in MANETs", International Journal of Ambient Systems and Applications (IJASA), Volume 2, Issue 3, 2014, Pages 1-9

A.V.Santhosh Babu received his B.Tech. degree in Information Technology, from K.S.Rangasamy College of Technology Anna University, Chennai. He obtained M.E. degree in Computer and Communication, from Sona College of Technology Anna University, Chennai. He has 7.5 years of teaching experience. At present, A.V.Santhosh Babu is working as an Assistant Professor in the Department of Information Technology at Sengunthar College of Engineering.

P. Meenakshi Devi received her B.E. degree in Computer Science and Engineering from Bharathiyar University. She obtained M.E. degree in Computer Science and Engineering from Madurai Kamaraj University, Madurai. She obtained her doctorate from Anna University Chennai. She has 20 years of teaching experience. She has presented papers in International and National Conferences. She has also published papers in National and International Journals. Her areas of interest include Digital Watermarking, Information Security and Cryptography. She is a life member of Indian Society for Technical Education. At present, P.Meenakshi Devi is working as a Professor in the Department of Information Technology at K. S. R. Institute for Engineering and Technology.