International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING

ISSN:2147-6799 www.ijisae.org Original Research Paper

Efficient Routing in Manets that Takes into Account Dropped Packets in Order to Conserve Energy

Nausheen Fathima [1], Dr. Mohd Abdul Bari [2], Dr. Sanjay [3]

Submitted: 08/09/2023 **Revised**: 22/10/2023 **Accepted**: 06/11/2023

Abstract: Mobile ad hoc networks are wireless networks that do not have a central server but instead function as a dispersed, multi-hop system. These networks are also known as mesh networks. MANETs are distinct from typical networks in several important respects, including the absence of a centralized coordinator, the dynamic nature of the network design, and the restricted access to network resources. MANETs can communicate thanks to a wireless radio transmission; nevertheless, because these networks are not physically secured, security measures can be implemented on them. In addition, because peer-to-peer networks are decentralized, they are an easy target for malicious actors that use the internet. As a result, a security solution is necessary to cope with the numerous attacks that may be launched against MANETs. It is difficult to maintain the batteries of MANET nodes charged while they are being used since the nodes themselves have restricted access to energy supplies. Therefore, giving energy efficiency together with security is a significant necessity in a distributed environment; numerous energy-efficient protocols and security protocols have been devised for MANETs, but these approaches are not ideal for the mission-critical applications that run on MANETs. Therefore, we want a unified solution that is capable of simultaneously satisfying our requirements for energy and security. It is difficult to establish the best secure and efficient way of routing between the source and the destination since there is no infrastructure, the network is peer-to-peer, and there are resource limits. When it comes to MANETs, we demonstrate that energy efficiency is just as crucial as secure routing, and we analyze the most recent research that has been conducted on the subject. The bottleneck that is generated by rejecting packets at the intermediate node is one of the issues that must be addressed when creating a system to handle this issue. The other obstacle is the lack of confidence in security solutions provided by third parties. As a result, we proposed a safe and energy-efficient routing protocol as a means of effectively mitigating harmful behaviors at the routing layer by carefully considering the factors that contribute to packet loss. The authentication that is offered by the approach that we have developed makes use of chaotic maps, which are far easier to calculate than RSA and ECC, both of which may be solved in polynomial time with the assistance of an advisor.

Keywords: *MANETs, Security, energy, routing, Packet dropping.*

1. Introduction

Mobile ad hoc networks [1] (MANETs) are autonomous adaptive system that consists of heterogeneous mobile nodes scattered in a radio communication region. Nodes in a MANET are free to move about and can be organized in any way that the network administrator sees fit. Because of the mobility of the nodes, the topology of the network is continuously evolving in ways that were not anticipated. If two nodes are within the range of radio communication with one another, then they can communicate directly with one another without the need for any intermediary nodes. Because of this, each node in a network is required to perform the function of a router by forwarding the packets generated by the other nodes. MANETs are largely distinguished by their capacity for self-organization and their ability to adapt to new environments.

Because of its one-of-a-kind properties, MANETs may be used for a wide variety of purposes across a variety of industries, including the military, healthcare, disaster recovery, government, and even civilian applications. At first, MANETs were created for use in military applications, namely to enable immediate and secure communication in conflict zones. In the future, this use of MANETs will pave the way for the development of MANETs in a wide variety of applications, including smart homes [2, resource sharing [3, conferencing [4, network games [5, and healthcare [6].

MANETs are becoming increasingly popular for use in a variety of applications, including monitoring of the environment and communication between vehicles. The use of MANETs in vehicular communication is a specialized subset of applications that is gaining a lot of traction. Work [6] described a system that may be used to give passengers information on location information. In addition to that, the work [7] offers to warn information to cars regarding the road surface, turnings, and traffic to ensure the safety of the passengers. MANETs have applications outside of the realm of vehicular communication as well, specifically in the field

[1] *Research Scholar, Kaling University, Raipur.*

[2] *Assocate Professor, HOD Computer Science Department ISL College of Engineering ,Hyderabad.*

[3] *Associate Professor, Department of Computer Science & Engineering, Kaling University, Raipur.*

of environmental monitoring. MANETs were established in the forest as part of the research conducted in work [8] to investigate the movement of carbon dioxide, with the goal of more precisely estimating the atmosphere of the forest. Work [9] built MANETs in farms to monitor soil moisture profiles in different depths and to track the motion of animals to lower the cost of managing the farms.

MANETs applications, such as those in the military, health care, and vehicular communication, are extremely sensitive and should be secure in communicating data. This is because even one incorrect message can cause a lot of problems, and one could even argue that it may directly relate to the lives of humans. Communication inside MANETs is feasible using a wireless communication channel, however, this does not provide any assurance of a person's physical safety and leaves them open to potential security risks. In addition, communication between peers is a basic vulnerability that may be exploited by attackers. Therefore, it requires a security system that can defend against the many different sorts of attacks that can be launched against MANETs.

Another difficulty presented by MANETs is that nodes only have a limited supply of energy, and it is extremely difficult to refuel the batteries of nodes in the middle of a mission, such as when they are deployed in a conflict zone. Since MANETs are peer-to-peer networks, the performance of the network is immediately affected by the compromise of a single node. Therefore, it is necessary to practice energy conservation to ensure that monitoring and detecting nodes, and the network as a whole, do not become inoperable.

When creating a security solution, one must pay careful attention to the resources that MANETs provide. Nodes in a MANET will use their energy to forward the packets that were generated by other nodes in the network. In addition, the operation of security algorithms consumes the energy of the nodes, which results in an additional burden being placed on the nodes of MANETs. MANETs are distinguished from wired networks by the presence of characteristics that are not found in the latter, such as wireless connectivity, dynamic network topology, and battery-powered devices. Because of this, the protocol for wired networks cannot function directly. In the following, we will illustrate why maintaining energy and security in MANETs is a crucial and difficult issue.

1. Mobile ad hoc networks (MANETs) are made up of battery-powered, heterogeneous mobile nodes; each node in a MANET must serve both as a host and a router to function properly. Power will be used up when nodes in MANETs forward packets on behalf of other nodes, which might be a big issue for some nodes in these networks.

2. Routing is the primary responsibility of the network layer, and it carries a heavy computational and communication workload.

3. The power consumption for transmission and reception of packets in conventional WaveLAN cards varied from 800 to 1200 mW, according to research that was published not too long ago [10].

4. It is vital to create a routing protocol that will be efficient with energy to be able to handle huge applications that are designed to last.

Security

1) Because MANETs are characterized by their decentralized nature, implementing security measures might be one of the most challenging parts of these networks.

2) Due to the limited battery capacity and processing powers of the nodes, MANETs are vulnerable to the deployment of security measures. This is because of their decentralized nature.

3) The security deployment does not have a clear direction or a defense plan in place.

It follows that applications of MANETs require a method that is both safe and effective in terms of the amount of energy it consumes. The provision of energy efficiency in conjunction with security is a major requirement in distributed environments; for MANETs, numerous energy efficient protocols [11] and numerous security protocols [12] have been developed; however, these schemes are not ideal for the applications described above. Therefore, a cohesive approach is required to adequately address both requirements (energy and security).

The Challenges That Come With Routing in MANETS

The provision of internet access is the primary focus of the design of wireless ad hoc networks.

The purpose of wireless ad hoc networks is to eliminate the requirement for any preexisting networks or other forms of infrastructure by providing users with the ability to connect to the internet at any time and from any location without restriction. The nodes that make up a MANET are free to move around and of varying types; also, the intelligence of the network is contained inside the nodes themselves. MANETs may be utilized in a wide variety of contexts, including but not limited to disaster assistance, the military, and law enforcement, thanks to characteristics like self-configuration and -maintenance. The problem of routing in MANETs is a particularly challenging one since there are so few resources available. When developing routing algorithms, making assumptions about cooperation among mobile nodes in a network puts the network at risk of security breaches and provides a foothold from which hostile attacks can be launched. In addition, the characteristics of MANETs, such as peer-to-peer network operations, an open medium, mobility, heterogeneity, and constrained resources, make it difficult to implement security solutions and lead to a wide variety of malicious attacks, such as the black hole, false report, and grey hole.

It is difficult to construct a way between communicating parts in a MANET because of the network's dynamic structure, mobility, and heterogeneity, which makes it difficult to establish an efficient path. There have been many different protocols designed to solve this problem, and the majority of them may be placed into one of three categories: reactive routing, proactive routing, or hybrid routing. Routing protocols that are proactive select the way in advance, whereas routing protocols that are reactive select the path only when it is required. The AODV protocol takes a reactive attitude when it comes to the routing process (Ad hoc on-demand distance vector). Within the context of this protocol, the minimum hop count and the maximum sequence number are both measured using units of measurement. As a consequence of this, malicious nodes can disrupt the routing path by asserting that they have knowledge of the shortest way and pulling all of the packets in the direction of their claim. During the early phases of a network's construction (during route discovery), when other malevolent nodes may be of assistance, those nodes may later pick which data to deliver and which data to ignore. In addition, other malicious nodes will report to the source that the data has not arrived, even though it has. When any one of these three damaging activities is carried out, packages are not delivered in the manner in which they were intended. As a consequence of this, the problem has to be solved by implementing a security system. The body of research that has been done on this topic has presented a variety of potential solutions to these security problems.

When it comes to MANETs, link layer protocols facilitate communication over a single hop, whereas network layer protocols make it possible to communicate over several hops. Even though this protocol operates on the assumption that all nodes are ready to collaborate to make communication easier, it is important to note that this is not necessarily the case in a competitive environment. Intruders will be able to sidestep a network protocol's functionality if they can find a way to subvert the protocol's requirements and go around them. Two of the key roles of network layer protocols are to locate the path that leads from the source to the destination and to pass data packets along that path. Both of these acts leave the network open to potential security threats. The majority of routing protocols select pathways according to predetermined criteria, such as those that need the fewest number of hops, the least amount of energy, the most available bandwidth, the least amount of latency, and so on. Other criteria may include: As a consequence of this, malicious nodes can divert traffic to themselves by asserting that the routing path that they choose is the most efficient possible according to the protocol metric. The "black hole" approach is an example of this type of attack. It is designed to pull in traffic by sending a very effective route replay message back to the source from which it originated. It is recommended that you send the packets through the rote replay receiver. When anything like this occurs, the black hole will just throw away the data. Initially, these nodes cooperate to carry out standard protocol activities, such as identifying the optimum path; however, later on, they begin to discard data selectively. An assault known as a "neighbor benefit attack" is one in which the attacker takes use of the advantages provided by the network's neighboring nodes without giving those advantages to the other nodes in the network. A misbehaving node will refuse to deliver neighbor packets since energy is a precious resource in MANETs and is used up throughout the data transmission process. As a result, the misbehaving node will drop them. The performance of the network layer is substantially hindered since the assault was coordinated in the process of route discovery but not in the process of data forwarding. However, other kinds of malicious nodes return a false replay to the source, suggesting that the data never reached its intended destination. This can happen while the data is being sent over a network. It is very necessary, to lessen the effect that misbehaving nodes have on the routing layer, and to recognize and separate problematic nodes from those that are, on the whole, useful.

All of the network layer attacks described above are connected to the practice of packet dropping. Despite this, there is a possibility of packet loss under specific circumstances because of the heterogeneity, mobility, limited resources, and inherent unpredictability of MANETs. As a consequence of this finding, we divided the reasons for lost packets in MANETs into the following categories.

a. A Crash

b. A Power Shortage

c. A Sluggish Transmission

d. An Overflowing Buffer (Fork in the Network)

e. Packet Header TTL Expired (Intermediate Node)

f. An assault originating from a black hole

g. An assault from a gray hole

h. Information that has been changed

i. Reduction in Particular Amount

Nodes in a MANET are dependent on the functionality of their neighbors since MANETs are multi-hop P2P networks. Collisions at the receiving end, whether they are clear or ambiguous, are the source of packet loss for this reason. These sorts of collisions are mostly attributable to an issue in MANETs known as the hidden node problem.

Receiver Collisions: A receiver collision happens when a source/neighbor node overhears that a packet is successfully forwarded to the next hop neighbor/destination node, but it is not, due to collision at the destination/neighbor node by concurrent another packet from another source/neighbor node. In other words, the source/neighbor node thinks that the packet is successfully forwarded, but it is not. In addition, this circumstance is not known to the source or neighbor node.

Ambiguous collisions: An ambiguous collision takes place when a source/neighbor node does not overhear that a packet has been successfully forwarded to the next hop neighbor/destination node. This is because another source/neighbor node is simultaneously transmitting packets in the direction of the source/neighbor node. But in this case, the packet was successfully delivered to the neighboring hop, which served as its final destination.

MANETs are infrastructure-less networks that have heterogeneous mobile nodes, and their buffers can overflow. Congestion is possible in this network environment at any node that is midway between the source and the destination of the data being sent. And because of this congestion, there is a significant rise in the number of packets that are lost, as well as an influence on the network's overall performance. Congestion control in infrastructure-based networks is handled by the transport layer protocols and operates independently of the protocols used for the other network layers. These methods, however, are not going to be applicable in a straightforward manner to infrastructure-less networks like MANETs. As a result of congestion being the primary cause of lost packets in MANETs, reducing congestion is one of the primary factors that should be addressed to decrease packet loss.

MANET is a heterogeneous network that permits the mobility of its nodes and makes communication feasible through a wireless medium. Transmission Power: Because nodes are heterogeneous, the radio communication area associated with each node is unique and varies depending on the strength of the node's wireless transmissions. If two communication nodes are not within radio range of one another, they will have to communicate with one another through the use of neighboring nodes as a relay. However, because of mobility, or the ability of a node to move from one location to another, packet loss can occur during communication if a neighboring node moves away from the region of communication.

Black hole attack: A black hole attack draws traffic toward itself by sending an efficient route replay message to the source. Black hole attacks are also known as traffic leaks. It is recommended that you send the packets through the rote replay receiver. After then, the black hole discards the packets.

An adversary node is sending out misleading reports on other nodes, which is a dishonest activity. It gives the impression to the source, through a bogus report, that packets have been successfully transported to their destination, whereas in reality, the packets are lost at neighboring nodes for unknown reasons.

Therefore, MANETs require a routing protocol that needs to mitigate the routing misbehavior attack by considering the reason behind the packet dropping. This is because there is a chance of packet dropping due to MANETs characteristics such as a distributed network with dynamic network topological architecture and an absence of central coordination. Therefore, the routing protocol must consider the reason behind the packet dropping. The provision of secure routing while taking into consideration the causes for packet dropping is one of the primary goals of the work that we have proposed; thus, a single procedure is highly desired in this regard. The remaining parts of the study are organized as follows: in the following section, we talk about related work on secure energy-efficient routing protocols, and in the following section, we tell about proposed work. The performance review and the conclusion bring our efforts to a close.

2. Related Work

The process of determining the path that will take one from one location to another most quickly and effectively is referred to as "routing." However, due to the nature of MANETs, this is extremely challenging.

Nevertheless, this is challenging with MANETs due to the following reasons:

1. There is no previous infrastructure

2. Restricted access to resources

3. The unpredictable structure of the network and the mobility of its nodes

4. There is a consistent risk that nodes may be hacked, which is one of the most significant security concerns.

A routing protocol that is focused on energy management is an essential component of design for a distributed system that has limited energy resources. Since the nodes that make up MANETs are powered by batteries, it is not possible to recharge or replace them on the battlefield, which is where they would be utilized. At the node, electricity is used for all three phases of the packet transfer process: transmission, receipt, and processing. Since MANETs is a peer-to-peer network, the performance of the entire network is significantly damaged if even the battery of a single node dies throughout the lifespan of the network. This can happen at any point in time. It has been suggested to increase the lifespan of networks using several different routing techniques. The majority of these procedures fall into one of three groups.

1. Determining the paths that would result in the fewest delays for the shipment of goods

2. To select the most effective and efficient routing pathways, a reliability-based routing algorithm is utilized.

3. Choosing paths that have a greater overall energy density

Protocols that are efficient in terms of energy path routing select the routing path that requires the least amount of energy for communication, and as a result, the total amount of energy that is consumed by all of the nodes in the network is decreased. To cut down on the amount of time spent on communication, reliability routing protocols select the routing path that results in the fewest retransmissions of control packets. Choose the route through the network that will take you past the greatest number of nodes containing energy. Utilizing different sorts of routing protocols in different kinds of networks can have both positive and negative effects on the network.

There is a multitude of routing protocols that have been developed to determine the best route between two or more points based on a variety of criteria, such as but not limited to, distance, hop count, delay, bandwidth, energy consumption, and security. These routing protocols have been developed in abundance. MANETs have been demonstrated to be effective in a variety of contexts, including the military, the medical industry, the environment, and vehicle communication. As a result, we believe that implementations of MANETs need to take into consideration both methods of energy savings and safety solutions. The majority of the requirements for communication may be satisfied through routing. For this reason, MANETs require a routing protocol that is both secure and efficient in terms of energy consumption. It is described how current routing approaches can increase both energy efficiency and data security at the same time.

The SREMCR [17] routing system is risk-free and effective in terms of the amount of energy it uses. It describes two distinct routes that can be taken to reach the destination. In the first place, it saves power by putting idle nodes to sleep and lowering the amount of energy that is consumed for active communication during the sending and receiving of packets. This helps to make the network run more efficiently. Second, the method offers security against an assault that is similar to a replay attack by utilizing a cryptographic checksum in conjunction with hashing. As a consequence of this, this strategy offers protection while also lowering overall energy use.

E-STAR [16] is a trustworthy and effective routing method that takes into consideration the amount of energy used. The trustworthiness of each node is evaluated, and a routing path is established by selecting the nodes that have the highest trustworthiness and enough energy to keep the route from failing as a result of excessive demands placed on the network. The value of trust is determined with the assistance of a hash function, and then it is validated by a trustworthy third party.

Distribution of keys that is efficient in terms of power consumption utilizing geographical data:

- It was pointed out in the study [15] that efficient management is required to offer secure and energy-efficient routing in a MANETs environment about cryptographic techniques and the physical placement of network nodes. This was emphasized as a necessity for successful management. It accomplishes this by making use of the geographical correlation that exists between the nodes of the network, which results in the creation of an energy-conscious and secure routing path. The distance between two nodes in space is the primary factor that affects whether or not they can utilize the same routing path to communicate and share data. According to the findings of this study, energy conservation takes place when geographical data about network nodes is taken into account throughout the process of realizing critical operations.

Table 1. Comparison between secure energy efficient routing protocols

Protocol	Energy Parameter	Security Parameter	Overhead	Attack Prevention	Possibility of node to become bottleneck	Environments	Architecture
SRMECR	Reduce active & In active communication energy	Hash Function	Multiple times hash verification	Replay attack	Yes	Simulation	Distributed & Collaborative
E-STAR	Sufficient energy	Hash Function	Depends on trusted party	Packet dropping, selfish	Yes	Simulation	Distributed & Collaborative
Secure Energy Efficient Routing based on geographic information	spatial correlation among the nodes	Geographical location	Geographical location is not a security parameter	No	Yes	Simulation	Highrarchical Architecture
Energy aware key distribution	Maximum Energy	Nodes behaviour based trust value	Nodes behaviour based trust value not always true for trust	Packet dropping attack	Yes	Simulation	Heterogeneous Multi hop

Energy Aware Trust Based Routing:- work [13], finds the energy-efficient and trustworthy route from source to destination to ensure secure data transmission based on considering the battery power, mobility, availability, and reliability of nodes. Energy Aware Trust Based Routing:- work [13], finds the most energy efficient & trustworthy route from source to destination to ensure secure data transmission. The behavior of individual nodes is used as a basis for the evaluation of trust. Work [14] created a path that prioritized conserving as much energy as possible while maintaining node trust. The trust value is determined by looking at the behavior of the nodes, as described in [13]. The comparison of routing tables based on their respective metrics is presented in Table 1.

Discussion: Protocols that are based on energy efficiency will cause the intermediate nodes to bottleneck, as routing is based on higher energy nodes path, and applying all the traffic through some priority-based nodes causes heavy traffic at a particular node buffer, and if this traffic is more than the node buffer capacity, then the packets will be dropped. This situation is known as a bottleneck intermediate node, and it is illustrated in figure 1 below. In the literature, all of the protocols do not take into account the situation of a bottleneck intermediate node in a network. If a particular node is accepting more traffic because it has high energy, this will cause congestion at the node's input buffer, which will result in the packets being dropped. According to Figure.1, if multiple sources select the route with an intermediate node 4, either because it has maximum energy or its better transmission capacity or because it contains other good resources, this causes node 4 to become a bottleneck intermediate node, which results in the dropping of packets and/or congestion in the network [18].

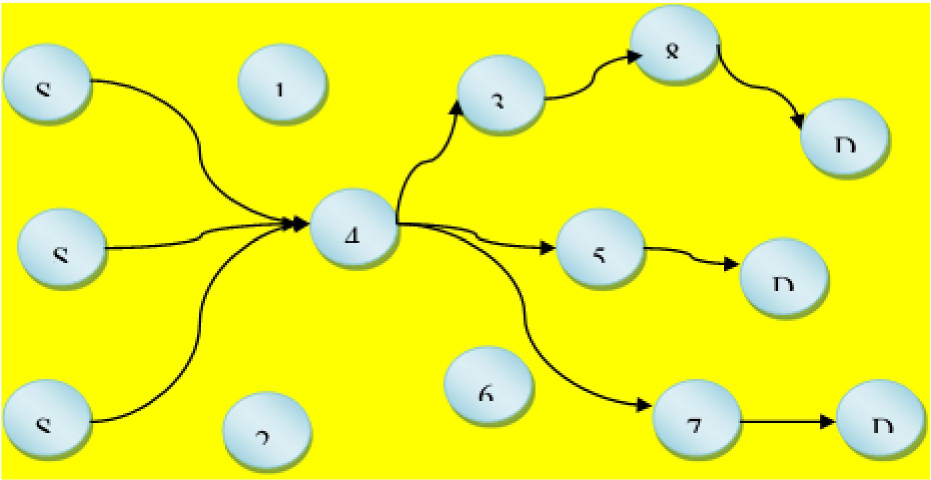


Fig 1 Bottleneck Intermediate node at node 4

It is difficult to provide security based on third-party authentication in MANETs since MANETs lack the infrastructure needed for traditional networks. In addition, providing security based on the communication behavior of individual nodes is not always reliable. This is because the communication behavior of individual nodes in MANETs is sometimes influenced by characteristics of the network, such as mobility, heterogeneity, and constrained resources. Similar to how a dropped packet is not necessarily caused by an attacker node, a dropped packet in a network might be caused by factors such as congestion, collision, a lack of energy and buffer capacity, or the expiration of the time to depart field in the packet header. Therefore, we build a routing protocol that ensures security by taking into consideration the causes of packet dropping. This protocol is called "Secure energy-efficient routing," and it is described in the section that comes after this one.

3. Prposed Work “Secure Energy Efficient Routing”

In the previous part, we discussed the difficulties that might arise while deploying MANETs as well as their potential benefits in terms of energy efficiency and security in the routing process. We have concluded that a single approach is required to solve both the issue of security and the issue of energy efficiency. In addition, we take a look at the recent developments in safe, energy-efficient, and effective routing protocols for MANETs. Because of this protocol, the intermediate node will eventually become a bottleneck, which will cause the routing path to get crowded and result in packet loss. Due to the lack of infrastructure present in MANETs, it is extremely challenging to implement a security system that relies on trusting a central third party. Furthermore, trusting a node only based on its communication behavior is not always accurate due to the mobility, heterogeneity, and constraint resources that it possesses. We have concluded that a single solution is highly wanted to design a routing protocol. This protocol should handle both security and energy efficiency by taking into consideration the bottleneck problem and by eliminating both node behavior and relay central third parties. Work [19] demonstrates that the problem of packet loss as a result of collisions may be solved by employing a dependable MAC protocol with collision avoidance, such as IEEE 802.11. It is possible to construct the routing protocol route selection metric in such a manner that it can eliminate the problem of discarding packets owing to insufficient energy, a lack of transmission power, or buffer overflow. The network layer's primary objective, should this protocol be included, is to provide a method for preventing attacks known as black holes and gray holes. For us to accomplish what we set out to do, we are each contributing to the task as follows.

1. A statistic for selecting the best route to take depending on the amount of current traffic and any remaining energy.[1]

2. Keeping an eye on the rate at which packets are decreasing.

3. Validation through the use of chaotic maps

In our earlier work [RER-SK,] we devised a way to accomplish energy efficiency by selecting the routing path based on metric values. This method was successful in achieving the goal. current traffic as well as the node's remaining energy by maximizing the packet processing capabilities of the node about the energy that is left over. The proposed work enhanced the lifespan of the network and prevented intermediate nodes from becoming bottleneck nodes, which resulted in a reduction in the number of packets that were dropped. This improvement is detailed in more detail in the next section.

3.1 A measure for the selection of the routing path that takes into account both the current traffic and the residual energy [RER-SK] [1]

Energy and latency are two characteristics that are strongly connected to the network lifespan and link stability in a distributed resource limitation environment. If these parameters are used more effectively, it may be possible to accomplish both link stability and network lifetime. MANETs are a type of peer-to-peer multi-hop network, in which each node in the network must perform the functions of both host and router. If the nodes that are interacting with one other are within radio range of one another, then they communicate directly with one another. If not, they rely on the intermediary node to get them to their final destination. Therefore, the resources of the intermediary node, such as its buffer, memory, and CPU, are utilized for communication. When a node in a network acts as a router and is responsible for forwarding and processing the packets of other nodes, that node's buffer space is used to temporarily store and process the packets. During a communication, a packet will be dropped at an intermediate node if that node is receiving several packets that are more than its input capacity. This condition is referred to as a bottleneck node. When a packet reaches the buffer of an intermediate node, it is required to proceed through a series of three stages before being allowed to leave the node

1. Packets stay in the input buffer queue until they reach the end of the queue, which is where decisions are made.

2. The decision module of an intermediate node retrieves the packet from the input buffer and decides based on the approach it employs (rouging decision)

3. Packets are stored in the node's output buffer until they are transferred from the node

Therefore, in our earlier work, the RER-SK routing protocol's primary objective was to control the conditions using data traffic to obtain improved network lifespan and link stability. We introduced the metric-optimized packet processing capacity of an intermediate device with the help of the knapsack algorithm to reduce the number of packets that were lost due to the buffer becoming overflowing. In this algorithm, we considered the controlling of the buffer by input traffic in addition to the residual energy of the node. The most important contribution made by the RER-SK routing protocol is presented below.

1. The optimization of the processing capability of an intermediate device for data packets in the presence of input traffic and residual energy.

2. Giving precedence to nodes depending on the ability of the nodes to handle metric data packets.

3. The selection of the routing path depends on the priority

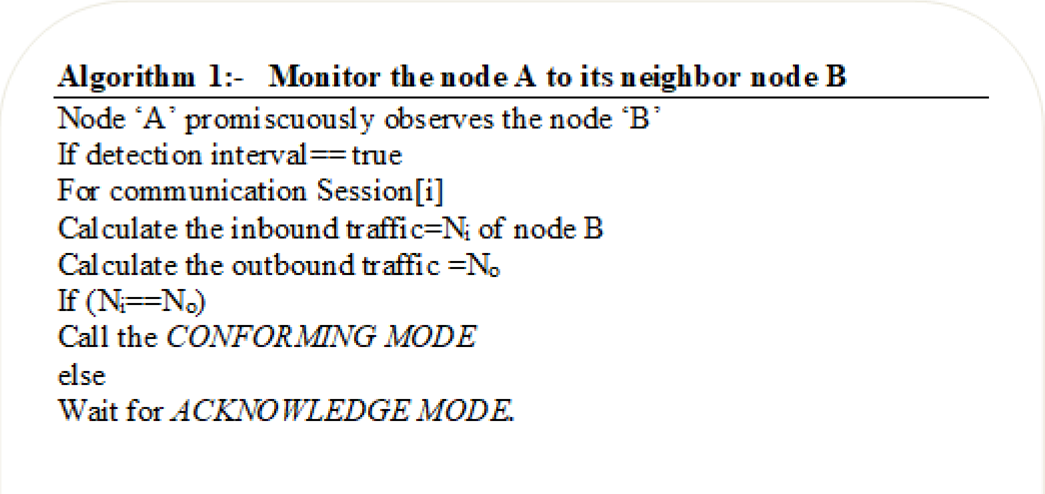
This routing technique reduces the likelihood of packets being lost due to insufficient power or an overflowing buffer; as a result, it eliminates the possibility of an input node serving as a bottleneck.

3.1 Monitoring

Monitoring is incorporated into our suggested model, the purpose of which is to lessen the burden that a trusted environment places on a computer network. Every node in a routing path will opportunistically monitor its next hop neighbor node regarding the number of data packets that it has transmitted, which is denoted by the phrase "several packets inbound to node I," in comparison to the number of packets that have been forwarded by the neighbor node, which is denoted by the phrase "several packets outbound form nodeN o." If all of the nodes between the source and the destination are cooperative with one another, then each node will discover the monitored information to be N (i=) N o, and communication will continue without any more steps being taken. If a node is promiscuously able to detect a difference between N i and N o and that difference is greater than the previously established threshold level, then that node will send a control message to the source node to tell it about the monitored node. The source node will then make a call to the Conforming mode to determine whether or not the indented node is malicious. Let's take into consideration the monitoring mode between A and B using algorithm 1.

3.2 Conforming

MANETs are infrastructure-less networks with resource-restricted environments; as a result, dropped packets may be the result of non-malicious actions such as insufficient energy, buffer size, or computational power. The conforming mode's purpose is to ensure that the monitored node has a valid cause for deleting packets. For route selection, we are making use of the routing protocol RER-SK, which is determined by the metric of current traffic as well as the residual energy of the node. As a result, there is no risk of packets being lost as a result of insufficient energy, transmission power, or buffer overflow. Work [19] demonstrates that the problem of packet loss due to collision may be solved by using a reliable MAC protocol. End-to-end acknowledgment combined with chaotic map-based digital signatures were able to successfully combat the issue of fake misbehavior attacks. The destination determines the time interval, and at the end of each time interval, it counts the number of data packets that were received by identical sources and sends the results back to the sources in the form of acknowledgments. The difference in the number of packets sent by the source and those received by the destination is compared to see if it is more than the threshold value. The source must first commence the new routing path before beginning to send the information through an alternate way. If a packet is lost due to a black hole or gray hole node, the source notifies all of the nodes within its range about the attacker node so that future communication may be directed away from it.



Algorithm 1:- Monitor the node A to its neighbor node B

```
Node 'A' promiscuously observes the node 'B'
If detection interval==true
For communication Session[i]
Calculate the inbound traffic=$N_i$ of node B
Calculate the outbound traffic =$N_o$
If ($N_i$==$N_o$)
Call the CONFORMING MODE
else
Wait for ACKNOWLEDGE MODE.
```

3.3 Chaotic map based digital signature

We utilize the digital signature that is based on the Chaotic Maps-Based Diffie-Hellman problem (CMBDHP) since it has a lower computational cost in comparison to RSA and ECC key generation, and because CMBDHP cannot be solved in a polynomial amount of time [20]. In our earlier work [18], we described how the session key agreement between two communicating entities may be derived from chaotic maps.

$$T_{n+1}(X) = 2X\, T_n(X) - T_{n-1}(X)\ ,\ n \geq 1 \ \ldots\ldots\ldots\ldots\ldots.1$$

The Chebyshev polynomial T n (X) is a polynomial in X of degree n, and it is represented by equation 1.

Work utilizes the semi-group property of Chebyshev polynomials to give authentication. The formula for this may be seen below.

$$T_n(X) = (2X\, T_{n-1}(X) - T_{n-2}(X))\ (\text{mod } N)\ldots\ldots\ldots\ldots\ldots\ldots\ldots.2$$

Where 'N' is a huge prime integer & n≥ 2, Xϵ (-∞, +∞).

If we give N, X, and T n (X), then it is theoretically impossible to determine the value of 'n' in equation (2). This type of issue is known as a Chaotic Maps-Based Discrete Logarithm problem [21].

$$T_n(T_m(X)) = T_m(T_n(X)) = T_{nm}(X)\ \ldots\ldots\ldots\ldots\ldots3$$

Where 'N' is a huge prime number, m, n >= 0& Xϵ (-∞, +∞).

If we give N, X, T n, and T m (X), then it is theoretically impossible to derive the value of 'T nm (X).' This is a property of Chebyshev polynomials that is referred to as the composition property. Entities in the network that communicate with one another agree on a session key through the application of equations (2,3)

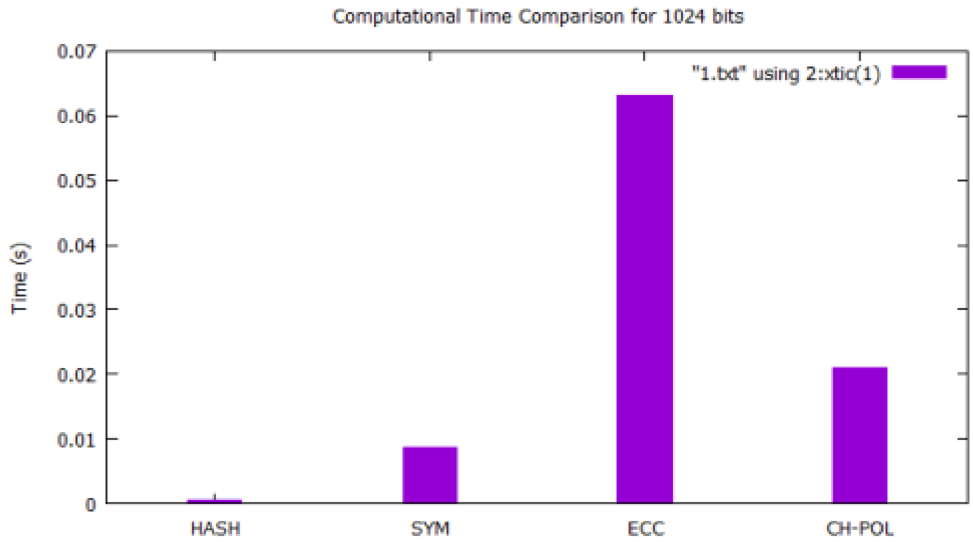


Fig.2 Computational Time Complexity of Cryptographically algorithms at 1024 bits

A destination must carry out the chaotic maps-based digital signature for the acknowledgment message of the destination to be authenticated. Compared to RSA and ECC, the Chebyshev polynomial has the advantages of a smaller key size, quicker computing and bandwidth, as well as memory and energy savings. Figure 2 presents a comparison of the amount of time required to compute ECC, the HASH function, the Symmetric method, and the Chebyshev polynomial using an input bit size of 1024 bits. The comparison between RSA and Chebyshev polynomials is presented in Table 2. Both figure 2 and table 2 make it abundantly evident that the amount of time required to compute a Chebyshev polynomial is far less than that required by ECC and RSA. Based on earlier work [18], we are mulling over the possibility of having two communicating entities agree on a session key that is based on chaotic maps. The destination incorporates the session key into the Ack message and determines the digest value with the assistance of a one-way hash function (H).

$$\mathrm{m} = \mathrm{Ack\ Xor\ Sesion\ Key}$$

$$\mathrm{d} = \mathrm{H(m)} \ldots\ldots\ldots\ldots\ldots 3$$

$$\mathrm{Digest\ message} = \mathrm{Ack} + \mathrm{d}$$

The packet is sent back to its sender after the digest message. The source needs to verify the accuracy of the message by using the following functions.

It takes out the Ack message and then appends the session key that it uses.

$$\mathrm{m}^1 = \mathrm{Ack\ Xor\ Sesion\ Key}$$

In addition to this, the one-way hash function applied

$$\mathrm{d}^1 = \mathrm{H}(\mathrm{m}^1)$$

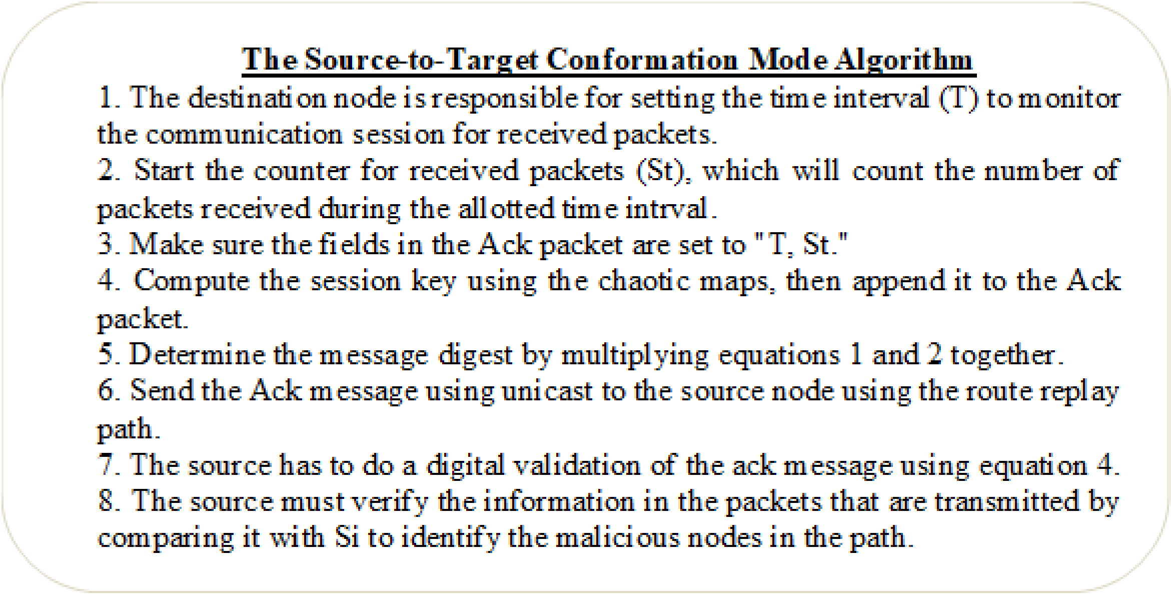
And it contrasts the value of d1 with the value that was received from the destination as d.

$$\mathrm{d}^1 = \mathrm{d} = ?\ \ldots\ldots\ldots\ldots\ldots 4$$

If they are going to match, then the source considers that the information was not altered while it was being sent.

Table 2. Comparison between RSA & Chaotic MAP (seconds)

Bits	RSA	Chaotic MAP
3	.000455561	.042253482
6	.000414247	.027530519
11	.016383556	.028748029
14	.864355422	.035146954
17	145.750098363	.038149370



The Source-to-Target Conformation Mode Algorithm

1. The destination node is responsible for setting the time interval (T) to monitor the communication session for received packets.
2. Start the counter for received packets (St), which will count the number of packets received during the allotted time intrval.
3. Make sure the fields in the Ack packet are set to "T, St."
4. Compute the session key using the chaotic maps, then append it to the Ack packet.
5. Determine the message digest by multiplying equations 1 and 2 together.
6. Send the Ack message using unicast to the source node using the route replay path.
7. The source has to do a digital validation of the ack message using equation 4.
8. The source must verify the information in the packets that are transmitted by comparing it with Si to identify the malicious nodes in the path.

4. Performance Analysis

The NS2.34 simulator was utilized for us to analyze the performance of our model and compare it with the secure knowledge approach in terms of throughput, packet loss, and routing overhead. In our simulation, we take into account a varying number of nodes using a mobility model with random waypoints and a halt duration of 20 meters per second. Every node has an IEEE 802.11 MAC card with data rates of 2 megabits per second and a battery with an initial capacity of 10 joules' worth of energy. The fixed radio transmission range is 250 meters. The power of reception is 300 milliwatts, while the power of transmission is 600 milliwatts. In conclusion, source nodes are responsible for producing CBR traffic with a packet size of 512 bytes. The duration of the simulation is one thousand seconds, and we took the average performance of three different scenarios. The following performance measures were taken into consideration while we were trying to measure the performance. The parameters of the simulation are presented in table 3.

Calculating how many data packets are sent from the origin to the destination in a certain length of time is one way to measure the performance of a network using a metric known as throughput. Packet Delivery Ratio is the ratio of the total number of data packets that were sent by the source to the total number of data packets that were received at the destination.

The ratio of the number of control packets that are transmitted for routing (including routing path discovery and maintaining the route) to the amount of actual data that is being transmitted in a network is referred to as the overhead.

Scenario 1: A reactive routing protocol with a rising number of nodes that do not contain a malicious node was the simulated scenario that was taken into consideration for our performance estimate. The second scenario is a reactive routing system that has an increasing number of malevolent nodes. Scenario 3: A malicious node is introduced into a secure knowledge algorithm [22] that has a rising number of nodes. Scenario 4: A proposed routing protocol with a growing number of malevolent nodes among the nodes in the network. In our simulation, there are three different kinds of nodes: normal nodes, which adhere to the routing specification and work together to route and forward data in communication; malicious nodes, which include black hole nodes, cooperative black hole nodes, multiple black hole nodes, and false misbehavior Ack nodes; and finally, hybrid nodes, which combine aspects of both normal and malicious nodes. The third kind of node is the one that discard packets owing to the bottleneck circumstance, which is caused by their energy or buffer.

Table 3. Simulation parameters of MANETs

Network Parameters	Values
Simulation Duration	1000 s
Number of Nodes	10-100
Link Layer Type	Logical Link
MAC type	802.11
Mobility model	Random way point
Routing	RER-SK, Proposed, SKA

Radio Communication	Two-Ray Ground
Queue Type	Drop-Tail priority
Energy	10j
Traffic	CBR
Area of Network	1500m x1 500m

Investigating the performance of a network with malicious nodes when it is experiencing a bottleneck scenario, such as several transmissions taking place across an intermediate node in a multi-hop environment, is our primary objective. As a result, we evaluate the packet delivery ratio in addition to the throughput and the overhead. Our previous work, RERSK, which is a reactive routing protocol and is based on metric-optimized packet processing capacity, is the first thing that we look into. While it performed well in scenario 1, it was unable to handle scenario 2 because malicious nodes dropped all of the packets that were sent to it. Because RER-SK performed well in multi-hop networks with bottleneck intermediate node conditions, however, it lacked any security implementations.

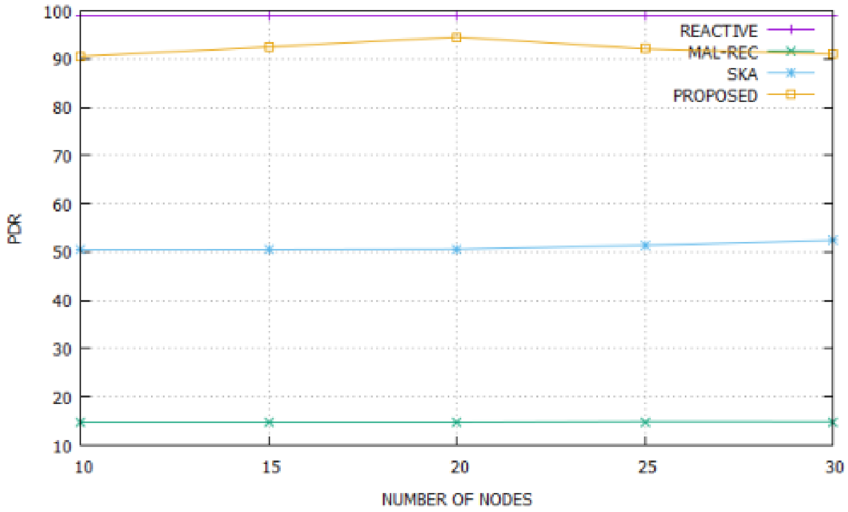


Fig.3 Packet Delivery Ratio of Proposed Approach compared with existing approaches

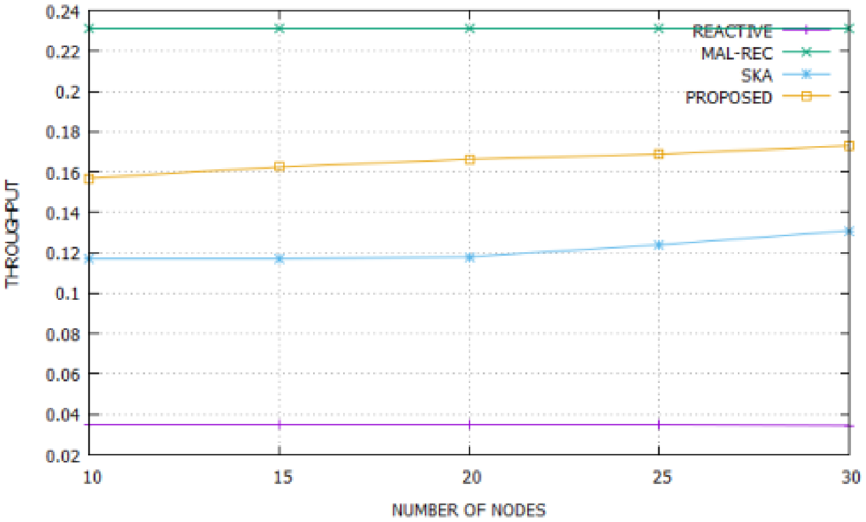


Fig.4 Throughput of Proposed Approach compared with existing approaches

Scenario 3 is an investigation of the performance of a secure knowledge method; it is based on AODV, and the hop count is used as the route-finding parameter.

It protects against the black hole attack, however, it can not do so very accurately since it cannot take into account the reasons why packets are dropped. The last scenario is our suggested effort; it is intended to reduce the impact of malicious nodes while also taking into account the reasons for packet loss. The outcomes of the simulations may be seen in figures 3, 4, and 5. The results reveal that our method is superior in terms of PDR and Throughput performance because it properly mitigates malicious nodes while incurring a lower level of overhead, as seen in figures 3 and 4. The findings of the proposed method are superior to those of the current ways on account of the proposed approach's precise identification of malicious activity, its route selection metric, and its consideration of the causes of packet dropping. In the current technique, route selection is determined by counting the number of hops between two points, which can lead to congestion on the routing path, buffer overflow, and overhead on particular node resources.

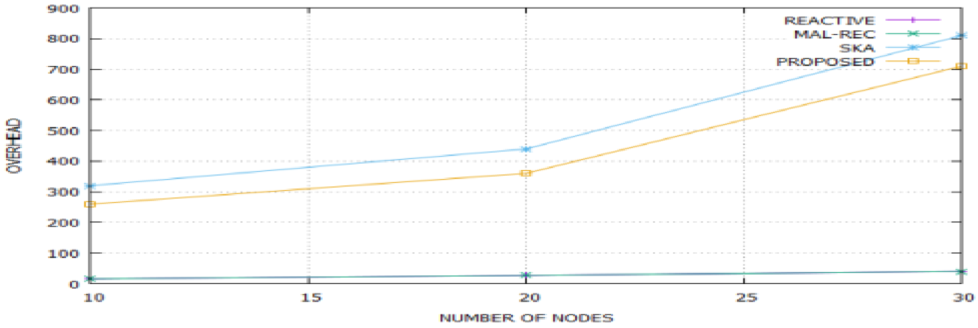


Fig.5 Overhead of Proposed Approach compared with existing approaches

4.1 Results Discussion

1. With the assistance of the route-finding measure known as "optimal packet processing capability of a node," we were able to solve the problem of packets being lost from nodes due to a shortage of energy and an overflowing buffer.

2. With the assistance of dependable MAC protocols like IEEE 802.11, we reduce the likelihood of packets being lost as a result of collisions.

3. We monitor in promiscuous mode, which enables us to identify and stop attacks including black holes and gray holes.

4. Through the use of authentication, we were able to solve the issue of attacks based on deceptive behavior.

5. We provide chaotic map-based authentication, which lowers the processing overhead associated with the authentication procedure.

5. Conclusion

MANETs, or infrastructure-less networks, are created specifically for use in very sensitive and important applications. The selection of a routing path that is both efficient and optimistic between the source and the destination is a highly tough element. Malicious actions in routing are mostly caused by the discarding of packets, however, a resource-constrained network environment can also cause packets to be dropped. In a multi-hop system, it is not necessarily accurate to label a node as malicious only on the basis that it drops packets when they exceed a given threshold level. As a result, based on our previous work, RER-SK, we presented a protocol to reduce the impact of rogue nodes in MANETs. It does this by taking into account the reasons why packets are being dropped, and as a result, it stops a trustworthy node from turning into a malicious one. The proposed architecture not only protects against malicious nodes but also boosts PDR and throughput while reducing the amount of overhead.

References

[1] Sana, Afreen Begum, Farheen Iqbal, and Arshad Ahmad Khan Mohammad. "Quality of service routing for multipath manets." In 2015 International Conference on Signal Processing and Communication Engineering Systems, pp. 426-431. IEEE, 2015.

[2] Siddiqua, Ayesha, Kotari Sridevi, and Arshad Ahmad Khan Mohammed. "Preventing black hole attacks in MANETs using secure knowledge algorithm." 2015 International Conference on Signal Processing and Communication Engineering Systems. IEEE, 2015.

[3] Sultana, Towheed, Arshad Ahmad Khan Mohammad, and Nikhil Gupta. "Importance of the Considering Bottleneck Intermediate Node During the Intrusion Detection in MANET." In Research in Intelligent and Computing in Engineering, pp. 205-213. Springer, Singapore, 2021.

[4] Mohammad, Arshad Ahmad Khan, Ali Mirza Mahmood, and Srikanth Vemuru. "Intentional and unintentional misbehaving node detection and prevention in mobile ad hoc network." International Journal of Hybrid Intelligence 1, no. 2-3 (2019): 239-267.

[5] Mohammad, Arshad Ahmad Khan, Ali Mirza Mahmood, and Srikanth Vemuru. "Energy-Aware Reliable Routing by Considering Current Residual Condition of Nodes in MANETs." In Soft Computing in Data Analytics, pp. 441-452. Springer, Singapore, 2019.

[6] Mohammad, Arshad Ahmad Khan, Ali Mirza, and Srikanth Vemuru. "Cluster based mutual authenticated key agreement based on chaotic maps for mobile ad hoc networks." Indian Journal of Science and Technology 9 (2016): 26.

[7] Mohammad, Arshad Ahmad Khan, Ali Mirza, and Mohammed Abdul Razzak. "Reactive energy aware routing selection based on knapsack algorithm (RER-SK)." In Emerging ICT for Bridging the Future-Proceedings of the 49th Annual Convention of the Computer Society of India CSI Volume 2, pp. 289-298. Springer, Cham, 2015.

[8] Mohammad, Arshad Ahmad Khan, Ali Mirza, and Srikanth Vemuru. "Analytical Model for Evaluating the Bottleneck Node in MANETs." Indian Journal of Science and Technology 9 (2016): 31.

[9] Mohammad, Arshad Ahmad Khan, Ali Mirza, and Srikanth Vemuru. "Energy aware routing for manets based on current processing state of nodes." Journal of Theoretical and Applied Information Technology 91, no. 2 (2016): 340.

[10] Abdul, Arif Mohammad, Arshad Ahmad Khan Mohammad, P. Venkat Reddy, Praveena Nuthakki, Rakesh Kancharla, Rahul Joshi, and N. Kannaiya Raja. "Enhancing Security of Mobile Cloud Computing by Trust-and Role-Based Access Control." *Scientific Programming* (2022).

[11] Mohammad, Arshad Ahmad Khan, Et Al. "Efficient Mobile Sink Location Placement By Residual Status In WSN To Enhance The Network Lifetime." Journal of Engineering Science and Technology 16.6 (2021): 4779-4790.

[12] Sastry, M. Kiran, Arshad Ahmad Khan Mohammad, and Mohammad Abdul Arif. "Optimized Energy-efficient Load Balance Routing Protocol for Wireless Mesh Networks." *International Journal of Advanced Computer Science and Applications* 12.8 (2021).

[13] Arshad Ahmad Khan Mohammad, Towheed Sultana" Evaluation Of Performance Degradation Due To The Presence Of Bottleneck Intermediate Node In Communication Path In Manet" International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249-8958 (Online), Volume-8 Issue-4, April 2019

[14] Mohammad Mohammad, Aleem Mohammed and C Atheeq, "Prior Bush Fire Identification Mechanism Based on Machine Learning Algorithms" International Journal of Artificial Intelligence and Applications, Vol.13, No.4, July 2022

[15] C Atheeq, M Munir Ahamed Rabbani, "CACK—A Counter Based Authenticated ACK to Mitigate Misbehaving Nodes from MANETs" Recent Advances in Computer Science and Communications 12, 2021.

[16] C Atheeq, M Munir Ahamed Rabbani, "Secure Data transmission in integrated internet MANETs based on effective trusted knowledge algorithm" Indian Journal of Science and Technology. Vol. 9 No. 47, Dec 2016

[17] C. Atheeq, Ahamed Rabbani, "Secure Intelligence Algorithm for data transmission in Integrated Internet MANET" International Journal of Computer Science and Applications, Vol. 14, No. 2, pp. 142 – 163, 2017

[18] Mohapatra, S. K. ., Patnaik, S. ., & Kumar Mohapatra, S. . (2023). An Enhanced Automated Epileptic Seizure Detection Using ANFIS, FFA and EPSO Algorithms . International Journal on Recent and Innovation Trends in Computing and Communication, 11(4s), 57–67. https://doi.org/10.17762/ijritcc.v11i4s.6307

[19] Diksha Siddhamshittiwar. (2017). An Efficient Power Optimized 32 bit BCD Adder Using Multi-Channel Technique. International Journal of New Practices in Management and Engineering, 6(02), 07 - 12. https://doi.org/10.17762/ijnpme.v6i02.57

[20] Dhabliya, D., Sharma, R. Cloud computing based mobile devices for distributed computing (2019) International Journal of Control and Automation, 12 (6 Special Issue), pp. 1-4.