International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5s
DOI: https://doi.org/10.17762/ijritcc.v11i5s.6643
***Article Received**: 19 February 2023 **Revised**: 02 April 2023 **Accepted**: 20 April 2023*

A Novel Method of Enhancing Security Solutions and Energy Efficiency of IoT Protocols

KDV Prasad[1], D Palanikkumar[2], Dankan Gowda V[3], Naziya Hussain[4], A. Azhagu Jaisudhan Pazhani[5], Anil Kumar N[6]
[1]Assistant Professor (Research), Symbiosis Institute of Business Management, Hyderabad, Symbiosis International (Deemed University), Pune, India. e-mail: Kdv.prasad@sibmhyd.edu.in
[2]Professor, Department of Computer Science and Engineering, Dr NGP Institute of Technology, Coimbatore, Tamilnadu, India. e-mail: palanikkumard@gmail.com
[3]Department of Electronics and Communication Engineering, BMS Institute of Technology and Management, Bangalore, Karnataka, India. e-mail: dankanies@gmail.com
[4]Associate Professor, School of Computers, IPS Academy, Indore, Madhya Pradesh, India. e-mail: naziyahussain@gmail.com
[5]Associate Professor, Department of Electronics and Communication Engineering, Ramco Institute of Technology, Rajapalayam, Tamilnadu, India. e-mail: alagujaisudhan@gmail.com
[6]Assistant Professor, Department of Electronics & Instrumentation Engineering, School of Engineering, Mohan Babu University (Erst while Sree Vidyanikethan Engineering College), Tirupati, Andhra Pradesh, India. e-mail: anilkumar.n@vidyanikethan.edu
Corresponding author: KDV Prasad, e-mail: Kdv.prasad@sibmhyd.edu.in

Abstract— Mobile Ad-hoc Networks (MANET's) are wireless networks that are capable of operating without any fixed infrastructure. MANET routing protocols must adhere to strict secrecy, integrity, availability and non-repudiation criteria. In MANETs, attacks are roughly categorised into two types: active and passive. An active attack attempts to modify or remove data being transferred across a network. On the other hand, passive attack does not modify or erase the data being sent over the network. The majority of routing protocols for MANETs were built with little regard for security and are therefore susceptible to a variety of assaults. Routing technologies such as AODV and dynamic source routing are quite common. Both however are susceptible to a variety of network layer attacks, including black holes, wormholes, rushing, byzantine, information disclosure. The mobility of the nodes and the open architecture in which the nodes are free to join or leave the network keep changing the topology of the network. The routing in such scenarios becomes a challenging task since it has to take into account the constraints of resources of mobile devices. In this an analysis of these protocols indicates that, though proactive routing protocols maintain a route to every destination and have low latency, they suffer from high routing overheads and inability to keep up with the dynamic topology in a large sized network. The reactive routing protocols in contrast have low routing overheads, better throughput and higher packet delivery ratio. AODVACO-PSO-DHKE Methodology boosts throughput by 10% while reducing routing overhead by 7%, latency by 8% and energy consumption by 5%. To avoid nodes always being on, a duty cycle procedure that's also paired with the hybrid method is used ACO-FDR PSO is applied to a 100-node network and NS-3 is used to measure various metrics such as throughput, latency, overhead, energy consumption and packet delivery ratio.

Keywords- Security, Throughput, Internet of Things, Energy Efficient, Mobile Ad-hoc Network, Pocket Delivery Ratio and reactive protocols.

I. INTRODUCTION

A seamless connectivity to users is provided by wireless networks regardless of their location. There are two kinds of wireless networks; one based on fixed infrastructure and the other is Ad hoc networks independent of a permanent infrastructure of any kind. The mobile devices in infrastructure based wireless networks are connected to fixed routers and gateways through a network of access points/base stations [1]. The mobile device in range of a base station remains connected to the network and on moving out of range is handed over to the next base station. A cellular network or a WiFi Local Area Network (LAN) is the example of infrastructure based network. The MANETs assume a trusted behaviour among nodes and are characterized by lack of centralized infrastructure, dynamic topology, open architecture, processing power, short range, and limited bandwidth, memory for storage and battery power [2]. The characteristics of MANETs have the following implications on the operations of MANETs: Multi-hop relaying: When source node and destination node are out of range, then, source node use their neighbour node as a relay nodes to send the packet from sender to receiver. Dynamic topology: MANET uses dynamic topology. Each node moves at different speeds from one place to other place and they dynamically establish routes among themselves.

Energy management: Nodes in MANET fully depend on battery power. Energy management plays a vital role in MANET. MANETs are finding increasing use in military, disaster management, search and rescue operations, surveillance networks, law enforcement operations, sensor

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5s
DOI: https://doi.org/10.17762/ijritcc.v11i5s.6643
***Article Received**: 19 February 2023 **Revised**: 02 April 2023 **Accepted**: 20 April 2023*

networks, vehicular ad hoc networks, public health, security and many commercial applications. In military the MANETs find extensive use to network various entities in hostile terrain or terrain where no infrastructure exists. It can be used to network devices carried by a small body of troops for surveillance and communication in an area which lacks networking infrastructure or can even network the entities of network-centric warfare in a battlefield in an enemy area where networking infrastructure is not available [3]. The MANETs can also be used to network a flotilla on high seas where no network is available. The disaster management and the emergency relief operations require networking of diverse teams, where existing infrastructure has been made inoperable; MANETs can effectively network all participating entities. The security agencies are often required to establish fast and secure network for law enforcement operations and the requirement can be met through ad hoc networks [4]. The machine-to-machine communication, sensor networks, smart home applications, connected cars, conferences and various business applications are some of the commercial applications of MANETs. The diverse applications of MANETs require quality of service, reliability and secure communication. Security of the networks is a priority, before these networks can be effectively employed in military and security related applications.

On-demand, Table-driven, and hybrid are the three types of routing protocols. The classification is clearly depicted in the Figure.1. Table-driven or PRP keep a routing table on each node. Routing tables are frequently sent across the network to keep the list of destinations and routes up to date. It always keeps a route open between any two hosts. A hybrid routing system combines proactive and reactive features to provide the best of both worlds. For the nodes in the routing zone, proactive routing protocols are employed. Outside of the routing zone, nodes must employ an in-band reactive routing protocol (IRRP). The security of MANETs is very important due to its increasing deployment in various applications and requires constant innovations and up gradations. Security was not the major design objective of most of these protocols and their emphasis was on simplicity and efficiency so that the routing protocols are light on resources [5].

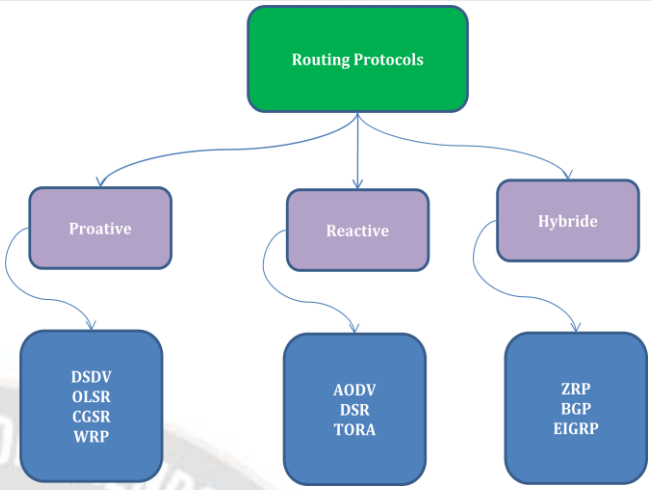

Figure.1: Categorization of protocols for routing.

The protocols were not addressing the issue of provision of security against often unpredictable attacks and making the protocol's reliability doubtful under such circumstances. In MANETs, there is no central mechanism for access control and traffic control and therefore it is hard to discriminate a malicious node from a legitimate node. An attacker therefore can easily gain access and disrupt the network operations. The security solutions for MANETs should therefore meet the following security objectives:

Confidentiality: It ensures that the authorized user only has access to the data and a malicious node is not able to eavesdrop and get the confidential information. The confidentiality is normally achieved by encryption of the data.

Availability: The requisite resources, like bandwidth and connectivity with other nodes of the network are available in timely manner to the legitimate nodes. Integrity: It guarantees that the data being transmitted has not undergone any modification or alteration by a malicious node.

As security becomes more of a concern, a secure communication channel must be established to allow mobile nodes to communicate in a antagonistic environment. A security environment is needed to overcome a set of challenges. Self-communicating devices don't need infrastructure to share information and constitute a MANET. Reducing network inefficiency is a major priority for computer experts who want to improve the central administration's network performance. ACO comes up with a higher-lasting energy-efficient route based on the ants' unique knowledge to fine-tune and is used to help the nodes to have a longer life by making sure that as little energy is wasted during transmission as possible [6]. Other techniques are examined to see whether they produced similar findings and also address the security concerns, including the inherent vulnerability of MANET's It is necessary to analyze network, security and the major attack types in order to provide network and information security. The major contributions of this work are: Enhancing

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5s
DOI: https://doi.org/10.17762/ijritcc.v11i5s.6643
***Article Received**: 19 February 2023 **Revised**: 02 April 2023 **Accepted**: 20 April 2023*

Security Solutions, Energy Efficient Transmission, Throughput enhancement and Identifying identify the vulnerabilities and types of attacks on routing protocols to analyze the impact of attacks and identify techniques for securing the routing protocols.

II. LITERATURE REVIEW

Securing of routing protocols for MANETs is an open research problem, many researchers have worked to identify the vulnerabilities and have proposed various techniques for securing the routing protocols. In [7] author's, compared the proactive and reactive routing protocols and have concluded that, the proactive protocols have lower route acquisition delay, since they maintain routes to all the nodes in their cache, but have requirements of large memory, greater processing power, more bandwidth, higher power and high control overheads. AODV, DSR, Ad-hoc On-demand Multi-path Distance Vector (AOMDV) and the proactive DSDV routing protocols decreased sharply with increasing traffic load. Maximum decrease was observed for the proactive protocols. PDR of all three reactive routing protocols was higher than that of the proactive routing protocol in the changing network topology. Proactive protocol, DSDV was not able to update the routes due to frequent

In [8] author's, observed that the hybrid routing protocols combine the proactive and reactive techniques to reduce the communication overheads and latency. The proactive routing protocol out of the three types had the worst PDR and throughput. The hybrid routing protocols had low communication overheads and latency but these advantages were dependent on the extent of the zone and zone dynamics. However, DSR had lesser NRL than that of AODV under all conditions. DSR showed maximum energy saving; however, the performance of DSR reduced considerably as compared to AODV at higher traffic loads. AODV outperformed DSR in all scenarios, except for small and medium size networks under low load conditions.

The protocols have been compared for the routing overheads, average delay per flow and PLR. DSDV had advantage over OLSR, and the reactive routing protocols in small and medium size networks with static or slow moving nodes. OLSR in contrast performed better in large and high density networks since the routing control traffic was minimized using Multi Point Relay (MPR) nodes. OLSR used smaller updates with an interval value of 1 sec as compared to DSDV, which used larger updates with interval value up to 5 seconds. The average delay per flow in OLSR was better than that of DSDV. DSDV exhibited the worst performance even as compared to reactive routing protocols in large and fast changing network topology. It had high PLR which can be attributed to its inability to update the routes in dynamic topology of the network.

In [9] author's discussed the attacks and their countermeasures across the complete stack of layers of MANETs. At the network layer, the authors identified the vulnerabilities of the routing process which led to attacks on proactive and reactive routing protocols. The defense mechanism suggested against passive attacks involved encryption of data. Customized solutions were proposed in the literature against every attack which may require additional hardware with nodes or modification of the protocols. In [10] author's, concluded that the security of MANETs was still in early stages and was an open challenge. The proposed solutions can typically provide security against few specific attacks and more research in this area was required. In [11] author's suggested the mitigation techniques for the various attacks, also conducted the survey of Intrusion Detection Systems (IDSs) for protecting MANETs from range of attacks.

In [12] author's discussed Flooding, Black-hole, Link-with holding, Link spoofing, Replay attack, Worm-hole and Colluding Miss-relay attacks on AODV and OLSR routing protocols. The authors suggested counter measures against each attack which were based on, monitoring the behaviour of the nodes and assigning trust values for flooding attack, re-confirming the authenticity of routing messages from neighbouring nodes for Black-hole attack, use of special hardware and cryptographic techniques for Link spoofing and Wormhole attack. The relative merits of each technique were compared and the authors concluded that the proposed solutions were not optimal when effectiveness and efficiency was considered. Therefore, the future research should explore the cost effectiveness of the solutions so as to make them suitable for MANETs. The types of attacks and the analysis of the attacks based on the type of protocols were presented by [13]. The authors analysed the effects of various attacks on the proactive and reactive routing protocols to determine if any protocol provided inherent protection against the attacks. The authors classified the attacks into, attack on sequence number, misdirection and DoS attacks. The Sequence number could be manipulated and flooding the network with spoofed packets with very high sequence number would discard the routing request from the legitimate node. The misdirection attacks could be launched by an attacker by various methods such as; impersonation as an existing node or a previously connected node, or through replay attacks or by attracting traffic towards it or deflecting traffic away from it or through Wormhole attack [14]. Different methods were used to exploit the vulnerabilities of routing protocols to launch such types of attacks. The DoS attacks were aimed at consuming the resources of the network by sending fake messages. The authors recommended authentication of originator and integrity check to prevent against most of the attacks and

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5s
DOI: https://doi.org/10.17762/ijritcc.v11i5s.6643
***Article Received**: 19 February 2023 **Revised**: 02 April 2023 **Accepted**: 20 April 2023*

concluded that proactive protocols were inherently more secure than reactive routing protocols.

The routing messages received from malicious nodes were discarded. The simulation results of the suggested technique for detection of Black-hole attack showed an improvement of 20 % in throughput and 40 % improvement in PDR.

The attacker in Sybil attack acquired multiple identities. Author's in [15] in their research proposed that the protection against the Sybil attack can be provided through authentication of a unique and unchangeable identity of the nodes through a Trusted Third Party (TTP). The authors proposed that the identity of the node can be tied down with the hardware of the node and suggested using the serial number of the hard disk as the unchangeable identity. The proposed technique authenticated the identities of the nodes with minimum use of TTP; however, it took much longer time for authentication of legitimate nodes. The authors were of the view that self-Certification Authority and distributed CA, though highly practical could not provide the security against Sybil attacks. A Central CA was required as TTP for issue of certificates for which more research was required for issue of keys and the certificates to the participating nodes.

To detect the malicious node using simultaneous identities attempting to launch a high bit rate attack, author's [16] proposed to track the movement of all the identities. The sender associated its location with every packet which was signed by its private key. The detection algorithm constructed the path each identity travels. The identities travelling similar paths were considered Sybil. The proposed technique required additional hardware in terms of directional antennas or GPS for determining the location of the nodes. The experimental results indicate 80% accuracy in detecting Sybil identities at slow speed of 5 mps; however, the accuracy dropped as the speed of the identities was increased.

The protocols in these broad categories even differ in their operation and have different characteristics. An in-depth study of routing protocols and the performance analysis of their characteristics are required to be undertaken[17]. The AODV and DSR are extensively used reactive routing protocols and the performance of these protocols has been compared in the literature. However, the performance analysis of these two protocols is not conclusive and requires further investigation under different scenarios. The vulnerabilities and attack on routing protocols were studied in the literature in piecemeal manner. A comprehensive study of the vulnerabilities of the routing protocols, the counter measures against the attacks exploiting the vulnerabilities and the techniques adopted by the existing secure routing protocols are important and is required to be studied. Security to the routing protocols is provided by a number of cryptographic techniques [18]. A detailed study of various techniques and a comparative analysis of various algorithms is required to be done.

To find the network's Black Hole, most current approaches look at the network from the perspective of its neighbours. However, this is less effective than dealing directly with the final node, since the journey from one source to another may not always be safe. The limited wireless range of the wireless node becomes yet another factor when considering this technique of neighbour negotiation since it is not a definite condition that nodes remain in range of each other.

III. SECURE AND EFFICIENT DATA TRANSMISSION

MANETs include several Sensor nodes and the placement of Sensor Nodes determines where information is sent. The nodes may move at will. ACO methods are used to optimize the efficient route construction utilizing the AODV routing protocol. Network sensors are clustered using Particle Swarm Optimization (PSO) algorithms. DHKE algorithms are used in sensor networks to protect individual packets. Due to their unique capacity to interact outside the node's immediate vicinity, MANETs are different from conventional wireless networks. When the destination is beyond a node's range of communication, the nodes work together to send the data there instead. As shown in Figure.2, the most extensively used and prevalent procedures in each of these groups are highlighted. A quick overview of these procedures is given, in this paper is for you. It has been decided to compare and contrast distinct types of protocols as well as the protocols within each category. RLEACH approached, a safe solution for LEACH clustering formed dynamically and regularly were developed [19]. A random pair-wish key orphan node was a big issue in RLEACH. Practical cryptography approach was proposed to solve the problem of orphan nodes. PSO and DHKE algorithms were used for clustering and security respectively. The protocols in this category differ from each other on the basis of number of tables maintained by each node and the algorithms for computing the routes. The changes in the network topology are communicated through routing update messages, which help in computing the latest routes.

IV. AODVACO-PSO-DHKE SYSTEM

In every ad-hoc wireless network, security is the primary issue. An innovative new solution for sensor network communication security, the AODVACO-PSO-DHKE is described in this research. In addition, the AODVACO-PSO-DHKE system will protect the data from a wide range of threats. As a result, DHKE requires less processing power while using less storage space. It's a Dynamic Optimization Problem for MANET routing since the search area varies over time. The routing policy determines which node must connect with which other on the route to get to the final node. In all, there are eight

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5s
DOI: https://doi.org/10.17762/ijritcc.v11i5s.6643
***Article Received**: 19 February 2023 **Revised**: 02 April 2023 **Accepted**: 20 April 2023*

critical phases to this system: Development of mobile nodes, clustering with PSO, selection of cluster heads based on node weight, an estimate of routers with AODVACO, the transmission of data to the cluster head, encryption with DHKE, receipt of data successfully, and finally, decryption [20]. Using the PSO-based clustering technique, the three steps need to be followed are: initializing the particles, calculating the fitness function, and updating their positions. PSO integrates local and global fitness in its search method. Predicting the current location of the legitimate data using particle changes and the associated data of nearby particles yields the ideal answer via iteration.

Two greatest esteems, for example, the original one, is used to update the particle on each iteration [21]. An individual particle can achieve the best Pbst. The global set of Pbst values yields a second-best value, which is denoted by gbst. A random deposition of particles and the use of the K-means clustering technique to get centroids is the first stage in particle initialization. PSO method was used to find the best possible locations for these points. In a fitness function, the particles' clustering scatter is considered. The created cluster scatter used as an input parameter for the fitness functions, provides a numerical value to verify the clustering scatters' accuracy.

$$F = \frac{1}{m}\sum_{i=1}^{m}\left\|O_j, D_j{}^{C_j}\right\| \quad (1)$$

The optimal particle for the cluster head is obtained via PSO. In order to get this information, it is necessary to calculate the distance between each node in the neighbourhood and the optimal centroid. D best is computed and the cluster that has the lowest D best is chosen

The D_best value is recalculated and the particle's location is updated as a result of the foregoing procedure [22]. The distance between the cluster's centre and its surrounding particles is used as a measure of the cluster's fitness. d best is equal to the minimum. The velocity of a particle has an effect on its location as given below:

Let $x_i(t)$ denote the particle position i in the search space at time step t. Then

$$x_i(t+1) = x_i(t) + v_i(t+1) \quad (2)$$

$$v_i(t) = v_i(t-1) + c_1 r_1\big(localbest(t) - x_i(t-1)\big) + c_2 r_2(globalbest(t) - x_i(t-1)) \quad (3)$$

Cluster networks of Sensor Nodes may be seen in Figure.3, clustered together. Each cluster network elects its CH based on the degree value that is the bare minimum. The cluster-role head collects data from nearby nodes and sends it to another CH on another network. Confirmation messages from the CHs give a time slot plan for their members to employ during the steady-state phase of their communication. Clustering changes dynamically in the "AODVACO-PSO-DHKE" approach, which is known as dynamic clustering.

V. ENERGY EFFICIENCY

As security becomes more of a concern, a secure communication channel must be established to allow mobile nodes to communicate in a antagonistic environment. The features of mobile adhoc networks offer a variety of potential security risks. Security features face nontrivial problems, such as open peer-to-peer networks [23]. Shared wireless media with rigorous network architecture restrictions on available resources, together with changing network topology, provide a difficult design challenge. A security environment is needed to overcome a set of challenges. Self-communicating devices don't need infrastructure to share information and constitute a MANET. Reducing network inefficiency is a major priority for computer experts who want to improve the central administration's network performance. A Collaborative Operating Committee (ACO) comes up with a higher-lasting energy-efficient route based on the ants' unique knowledge to fine-tune the nodes in the network. MANETs is a kind of multi-hop network, built from the ground up with no previous infrastructure in place. The major difficulty system security designer’s face is due to the wireless and dispersed nature of the system. The emphasis placed on MANET security issues has dramatically increased in the last few years. Last but not least, by dividing a message into N pieces and spreading them over the routes, a limited degree of transmission redundancy is provided with the goal of enabling. Each bit is protected by an integrity and replay-proof cryptographic header that verifies and tracks where it is coming from, as well as who created it. When one or more items are delivered, the destination includes an acknowledgment which notifies the source of which items arrived undamaged, and thus routes. To promote the strength of the feedback system, the acknowledgement In case the source receives no more than M pieces, the source retransmits the remaining pieces using all the previously established routes. If the protocol recognizes that a small percentage of recognized pieces is insufficient, or if a substantial percentage throughout the path is set, among other things, if this is not the case, the computer will transmit the next message in the queue to the recipient.

VI. ANALYSIS AND PREVENTION

The TCP/IP protocol suite is used by MANETs, and the underlying layers adhere to IEEE 802.11 specifications. MANET-specific routing protocols are used at the network layer, where most of the differences may be found. To perform its functions of transmission of messages, neighboring relationship formation and collection of route information in routing databases, the routing protocols exchange control messages. The routing protocols are subjected to threats at various levels. An attacker may attack the control messages to break the neighboring relationship or may attack the routing

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5s
DOI: https://doi.org/10.17762/ijritcc.v11i5s.6643
***Article Received**: 19 February 2023 **Revised**: 02 April 2023 **Accepted**: 20 April 2023*

control messages to disrupt the routing process. There are a number of ways that an attacker might disrupt adjacent relationships in a routing protocol, such as by modifying 'Hello' messages or by altering Topology Control (TC) messages. The RREQ, RREP, and RERR control messages in the Reactive Routing protocol may also be attacked in the same way. An outsider or a Byzantine node might be the perpetrator. It is possible for an outsider to serve as both a source and an intermediary node. To launch an attack, it may either use its own address, another node's address, or any other address it chooses. It is possible for a malicious node to alter or replay received packets, causing a route interruption or denial of service, if it is functioning as an intermediary node. Byzantine nodes on the other hand are faulty, misconfigured or subverted nodes which are legitimate participants of routing process. The threat consequences due to actions of the attackers compromise the correct behavior of the routing process which can damage the data traffic intended for a particular node. Figure.5. depicts the taxonomy of attacks which are explained as under:

By monitoring/intercepting network traffic, a passive attacker may figure out what is going on. important and critical information without disturbing the routing process. The information could be about the topology, location of important nodes or the identity of the nodes, type of data exchanged on the network. Some of the prominent passive attacks are as follows:

Sniffing Attack. The wireless transmission over the MANET can be heard by every device equipped with a receiver and within a range. An attacker monitors/records the routing exchange control messages on the network. The consequences of sniffing depend on the transmission range of nodes, geographical distribution of nodes, location of the attacker, type of routing protocol and the information.

Traffic Analysis. An attacker can listen to the data traffic that is flowing through the network and can deduce the routing information by analyzing the amount of data transmitted, communication pattern and the type of data transmission. The analysis can be carried out even if the data is encrypted and can reveal the location of important nodes which can be targeted.

Spoofing Attack. In this type of attack, the attacker assumes the identity of a legitimate node. Spoofing in itself does not constitute an attack but can be used to launch other attacks. The consequences of spoofing are that an attacker will be able to know the routing information and also can disrupt the neighboring relationship with other nodes.

Routing protocol flaws, attacks that make use of these vulnerabilities, and methods to prevent these attacks are all covered in this paper. It can be observed that no single method can provide security against all attacks. The vulnerabilities from external attackers and internal attackers have to be addressed in a separate manner. Some of the secure versions of routing protocols have been developed and proposed in the literature. However, none of these protocols has been able to provide protection against all types attacks. Moreover, the secure version of the routing protocols excessively uses the cryptographic techniques which add excessive computation load on the resource constrained nodes. The requirement is therefore to devise a light weight cryptographic technique which meets the goals of security. A Black Hole attack may be more damaging to the AODV protocol than to the OLSR protocol, according to our investigation.

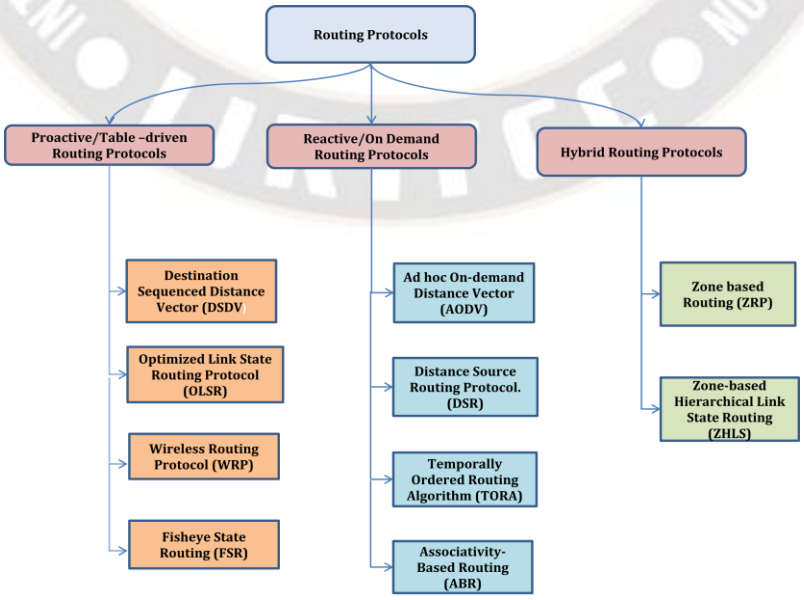

Figure.2: Types of Routing Protocols

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5s
DOI: https://doi.org/10.17762/ijritcc.v11i5s.6643
***Article Received**: 19 February 2023 **Revised**: 02 April 2023 **Accepted**: 20 April 2023*

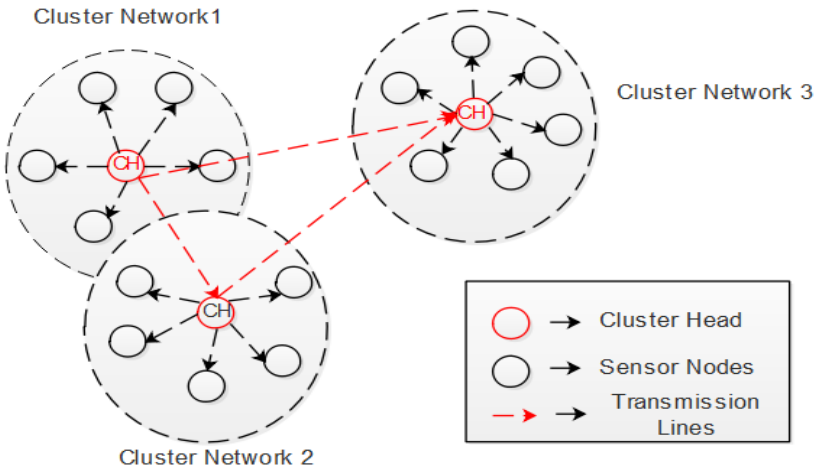

Figure.3: Basic Clustering in Mobile ad-hoc network

Table.1: Comparative Analysis of Proactive Routing Protocols

Parameter	DSDV	OLSR	WRP	FSR
Routing Algorithm	Distributed Bellman-Ford	Optimized Link State Routing	Improved distributed Bellman-Ford	Link State routing algorithm
Routing Structure	Flat	Flat	Flat	Hierarchical
Route Metric	Shortest Path	Shortest Path	Shortest Path	Shortest Path
Number of Tables	2	3	4	3 and a List
Frequency of Updates	Periodic and as required on occurrence	Periodic	Periodic	Periodic exchange of updates more frequent in nearby nodes. Less frequent for nodes far apart.
Control Overheads	High	Low	High	Low
Scalability	Small and medium Size	Large and Dense Network	Small and medium Size	Large and Dense Networks
Convergence of routes	Slow as compared to WRP	Fast	Fast	Fast
Loop-free	Sequence number prevents loops	Link State entry prevents loops	Records Predecessor and Successor nodes. Additional overheads are incurred for consistency checking.	Link State entry prevents loop.

Table.2. Comparative Analysis of Reactive Routing Protocols

Parameter	AODV	DSR	TORA	ABR
Routing Algorithm	Distance Vector	Source Routing	Link Reversal	Degree of Association Stability.
Multiple Routes	No	Yes	Yes	No
Route Metric	Shortest path	Shortest path	Height	Link Associativity
Control Traffic Volume	Low Overheads	Overheads increase with the size of the network	Large Overheads due to maintenance of height and status of connected link.	Large overhead. due to beacon updates.
Scalability	Small, medium and Large Dense Networks	Small and Medium Networks	Large Dense Networks	Small and Medium networks.
Link Failure Information	Flood, Erase Route and inform Source Node	Flood, Erase Route and inform Source Node	Link Reversal and Route Repair	Local Broadcast Query.
Loop Free	Yes Sequence number	Yes Checking root record field,	Yes Link State entry prevents loop	Yes Link State entry prevents loop.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5s
DOI: https://doi.org/10.17762/ijritcc.v11i5s.6643
Article Received: 19 February 2023 Revised: 02 April 2023 Accepted: 20 April 2023

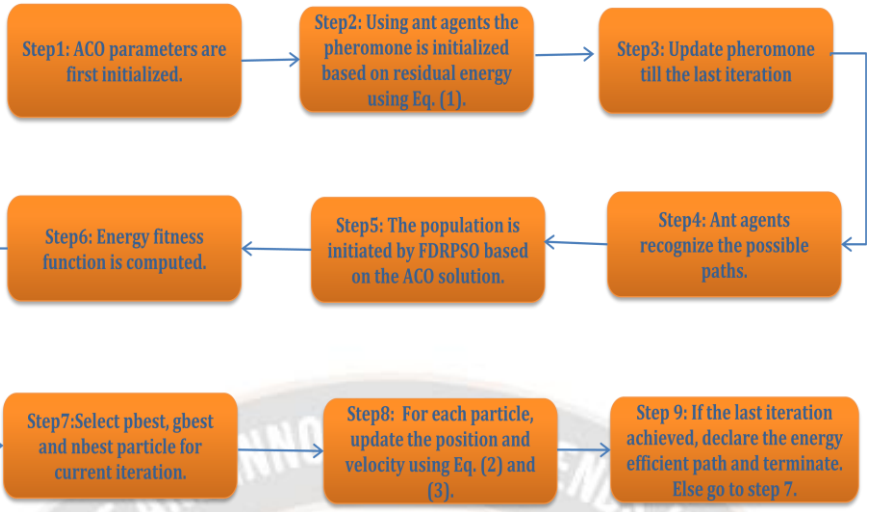

Figure.4: Steps of ACO-FDR PSO

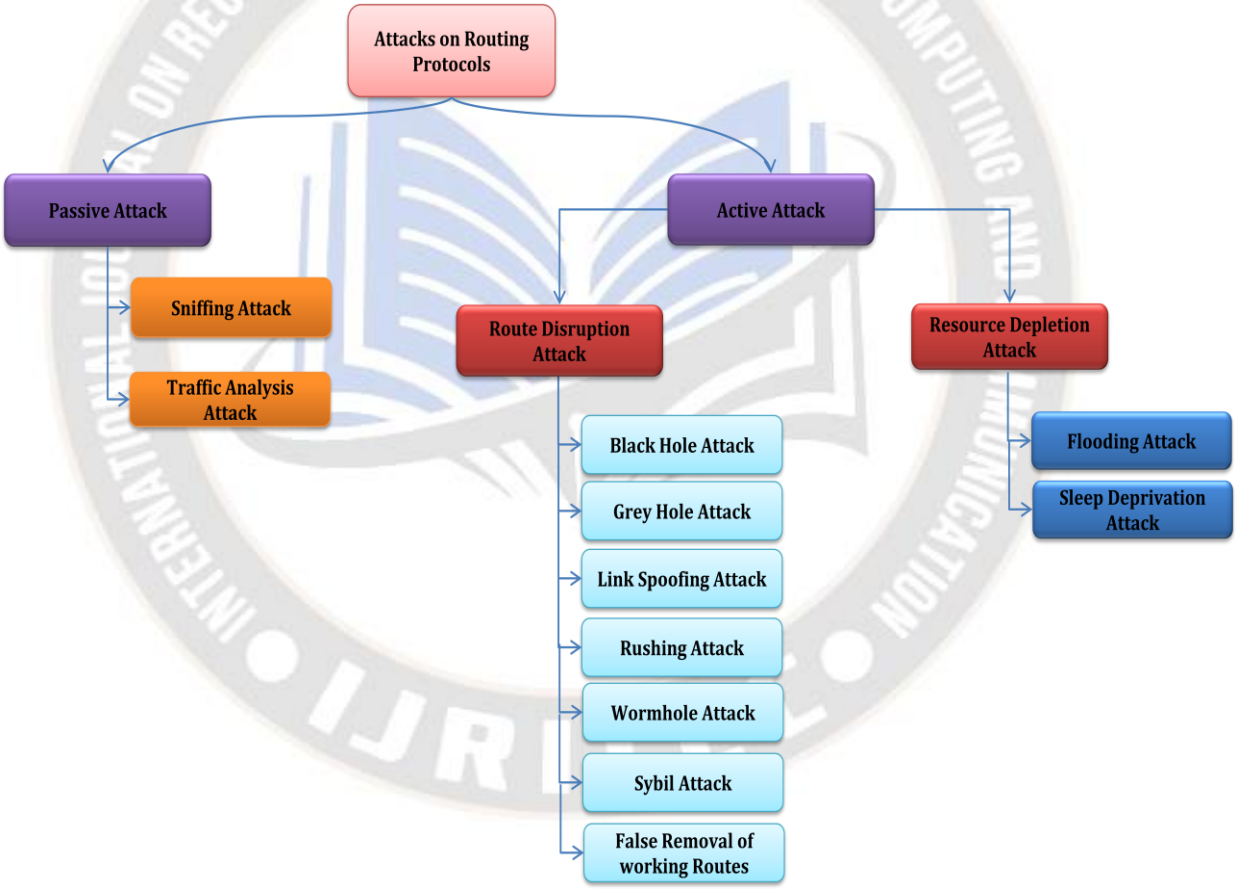

Figure.5: Classification of Attacks on Routing Protocols

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5s
DOI: https://doi.org/10.17762/ijritcc.v11i5s.6643
***Article Received**: 19 February 2023 **Revised**: 02 April 2023 **Accepted**: 20 April 2023*

VII. RESULTS AND DISCUSSION

Data transmission is accomplished by utilizing an efficient clustering and routing technique that uses the AODV routing protocol with the ACO optimization algorithm written in NS2. The I7 machine with 8 GB of RAM is used for all of the tasks. PSO algorithm and the DHKE method are both used to find the most efficient way for wireless mobile nodes to transmit data securely. AODV-ACO and DHKE algorithm findings are presented in this section in further depth. The nodes' communications are secure thanks to the AODV-ACO-PSO-DHKE method. Throughput, routing overhead, latency and energy usage are all taken into account when calculating the performance. A reduction in routing overhead results in an improvement in throughput and PDR.

$$Throughput = \frac{Total\ packets\ received\ at\ the\ destination}{Node\ total\ Simulation\ time}$$

$$Roughting\ Overhead = \frac{Total\ no.of\ routing\ packets}{Total\ no.of\ delivered\ data\ packets}$$

Energy consumption: The enormous quantity of incoming energy usage is mirrored by the enormous number of hops.

As shown in the simulation results, AODVACO-PSO-DHKE Methodology improves throughput by 10% in comparison to AODV-PSO Methodology [16]. AODV-PSO Methodology has a routing overhead of 7 percent less than AODVACO-PSO-DHKE. the DHKE method and the AODVACO-PSO method are compared. AODVACO-PSO-DHKE reduces delay by 8% compared to AODV-PSO Methodology. AODVACO-PSO-DHKE Methodology reduces energy consumption by 5% in comparison to AODV-PSO Methodology. Figure.6. shows the comparison of nodes versus throughput for AODV-ACO-PSO-DHKE and AODV-PSO.

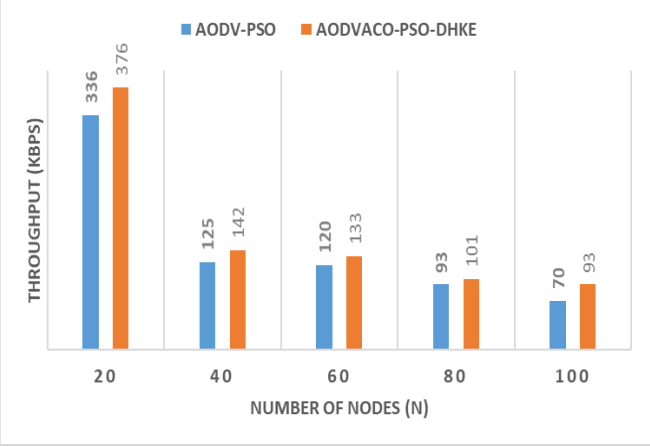

Figure.6. Node vs. Throughput

Figure.7. shows the comparison of AODV-ACO-PSO-DHKE vs. AODV-PSO in terms of nodes and routing overhead. When comparing the AODV-ACO-PSO-DHKE technique to the AODV-PSO method, the routing overhead is reduced by adjusting the number of nodes.

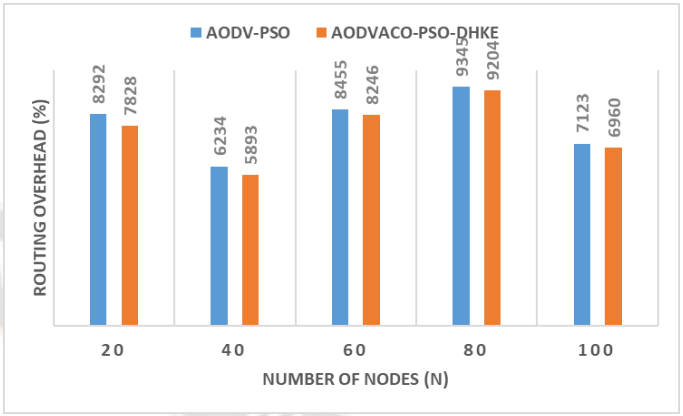

Figure.7. Node vs. routing overhead

PSO-DHKE and AODV-PSO are shown in Figure.8., which compares the number of nodes and the latency between the two protocols.

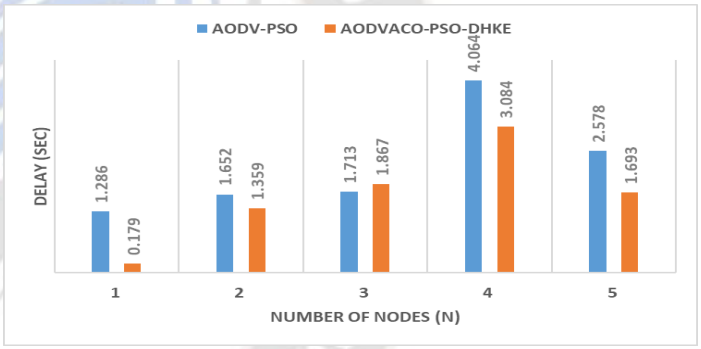

Figure.8. Node vs. delay

For AODV-PSO and AODV-ACO-DHKE, the node vs. energy comparison is shown in Figure.9. When AODV-ACO-PSO-DHKE technique is compared to AODV-PSO method, the energy consumption is reduced by adjusting number of nodes.

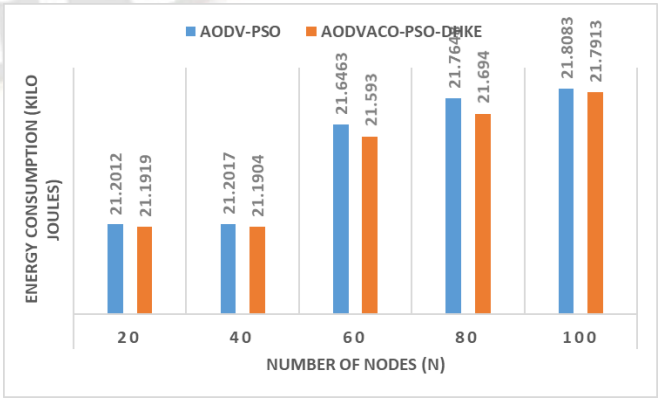

Figure.9. Node vs. Energy Consumption

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5s
DOI: https://doi.org/10.17762/ijritcc.v11i5s.6643
***Article Received**: 19 February 2023 **Revised**: 02 April 2023 **Accepted**: 20 April 2023*

By lowering the amount of overhead, time delay and energy used during the routing process, AODVACO-PSO-DHKE approaches have proven useful in sensor networks for safeguarding data packets from source to destination.

As a result of the M-TCFPA approach's reduced communication latency, the route discovery phase experiences shorter path identification and fewer control packet transfers. There is a significant difference in efficacy between M-TCFPA and TBSMR.

Table.3. Comparative analysis of M-TCFPA

Performances	Method	Number of Nodes				
		10	50	100	150	200
PDR (%)	TBSMR [20]	98	97	95	92	90
	M-TCFPA	99.77	99.37	98.50	99.04	98.85
PLR (%)	TBSMR [20]	2	3	5	8	10
	M-TCFPA	0.22	0.62	1.49	0.95	1.14
Throughput (kbps)	TBSMR [20]	510	500	470	440	410
	M-TCFPA	1090.36	1086.1	1077.85	1083.72	1083.27
AEED (sec)	TBSMR [20]	0.1	0.15	0.2	0.25	0.3
	M-TCFPA	0.024	0.027	0.038	0.060	0.070

Table.3. compares the TBSMR [20] and M-TCFPA [21] methods in terms of accuracy. Changing the number of sensor nodes used, i.e. 10, 50, 100, 150, and 200, allows comparisons to be made between different numbers of sensor nodes. Based on Table 2, it's clear that the M-TCFPA method [20] beats the TBSMR method. Only trust, traffic, and residual energy values were taken into account by the TBSMR [20] during data transmission. When transferring data packets, this TBSMR [20] does not take distance under account. There is a delay in transmitting the data packets because of this. The M-TCFPA approach makes use of trust and integrity to make sure the nodes are reliable and the data they exchange is accurate. As a result, the M-TCFPA method's data delivery is improved while transmission latency is reduced.

VIII.CONCLUSION

MANET's is an alternate wireless network architecture which is finding increasing use in defence, law enforcement, disaster management and commercial applications. This research work includes Enhancing Security Solutions, Energy Efficient Transmission, Throughput enhancement and Identifying the vulnerabilities. Ad-hoc networks may employ the "AODVACO-PSO-DHKE" approach for secure data transfer. As a result, the AODV routing protocol with ACO optimization is utilized for efficient data transfer. PSO Clustering is used to keep each node's energy consumption under control. DHKE approach is used to secure data transfer from source to destination. Regarding energy usage and throughput, the new approach is superior to the current method. Because of this, AODVACO-PSO-throughput DHKE's improves by 10% compared to AODV-PSO Methodology, while routing overhead and latency are down by 8%, and the energy consumption is down by 5% using AODVACO-PSO-DHKE. Performance analyses of routing protocols, the vulnerabilities of the routing protocols which lead to several attacks have been reviewed. Several proposed security enhancements for the routing protocols have been examined. Most of the existing routing protocols are developed to mitigate various network layer attacks such as black hole, wormhole and rushing attack used cryptography based technique and as well as trust based techniques. This may add additional overhead and processing time. It also decreases the throughput of the network. Our research is focused on developing secure routing protocol to mitigate various network layer attacks with less cryptographic techniques. The parameters considered are PDR, throughput, delay, packet loss and routing overhead. In order to construct a safe cluster-based routing system that can effectively transfer data, the M-TCFPA technique is proposed. Data transmission on the MANET can be improved by using the K-means clustering technique. Based on trust, integrity factor, residual energy, distance, and the M-TCFPA method's selection criteria, the best CH and routing are determined.

REFERENCES

[1]. S Sarkar and R Datta, A Secure and Energy-efficient Stochastic Multipath Routing for Self-organized Mobile Ad Hoc Networks, Ad Hoc Networks, 37 (2019), 209-227.

[2]. L Abusalah, A Khokhar, and Mohsen Guizani, A Survey of Secure Mobile Ad Hoc Routing Protocols, IEEE Communications Surveys & Tutorials, **10** (4) (2018), 78-93.

[3]. M. Swathi Pai, M. Shruthi and B. Naveen K, "Internet of Things: A Survey on Devices, Ecosystem, Components and Communication Protocols," 2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA), 2020, pp. 611-616, doi: 10.1109/ICECA49313.2020.9297458.

[4]. S. B. Sridhara, K. B. Naveen, M. Ramesha, and G. N. Pai, "Internet of things: Internet revolution, impact, technology road map and features," Adv. Math. Sci. J., vol. 9, no. 7, pp. 4405–4414, 2020, doi: 10.37418/amsj.9.7.11.

[5]. C. Toh, H.Cobb and D. Scott. "Performance Evaluation of Battery-Life-Aware Routing Schemes for Wireless Ad Hoc Networks", Proc. IEEE International Conference on Communication, Helsinki, Finland, pp.2824-2829, 2018.

[6]. Shivashankar, and S. Mehta, "MANET topology for disaster management using wireless sensor network," in International Conference on Communication and Signal Processing, ICCSP

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 5s
DOI: https://doi.org/10.17762/ijritcc.v11i5s.6643
***Article Received**: 19 February 2023 **Revised**: 02 April 2023 **Accepted**: 20 April 2023*

2016, 2016, pp. 0736–0740, doi: 10.1109/ICCSP.2016.7754242

[7]. Jayashri N, Veeresh Rampur, Durgaprasad Gangodkar, Abirami M, Balarengadurai C, Anil Kumar N, Improved block chain system for high secured IoT integrated supply chain, Measurement: Sensors, Volume 25, 2023, 100633.

[8]. Rajashanthi, M. and Valarmathi, K.: A Secure Trusted Multipath Routing and Optimal Fuzzy Logic for Enhancing QoS in MANETs. Wireless Personal Communications, 112, 75-90 (2020).

[9]. B.S., Ramesh Naidu, P., Sridhara, S.B. (2023). Internet of Things and Cognitive Radio Networks: Applications, Challenges and Future. In: Yadav, S., Chaudhary, K., Gahlot, A., Arya, Y., Dahiya, A., Garg, N. (eds) Recent Advances in Metrology . Lecture Notes in Electrical Engineering, vol 906. Springer, Singapore. https://doi.org/10.1007/978-981-19-2468-2_3.

[10]. S. B. M, P. Pavankumar, N. K. Darwante, "Performance Monitoring and Dynamic Scaling Algorithm for Queue Based Internet of Things," 2022 International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES), 2022, pp. 1-7, doi: 10.1109/ICSES55317.2022.9914108.

[11]. A. Singla, N. Sharma, "IoT Group Key Management using Incremental Gaussian Mixture Model," 2022 3rd International Conference on Electronics and Sustainable Communication Systems (ICESC), 2022, pp. 469-474, doi: 10.1109/ICESC54411.2022.9885644.

[12]. S. Reddy P, P. S. Patwal, "Data Analytics and Cloud-Based Platform for Internet of Things Applications in Smart Cities," 2022 International Conference on Industry 4.0 Technology (I4Tech), 2022, pp. 1-6, doi: 10.1109/I4Tech55392.2022.9952780.

[13]. A. Sharma, K. S and M. R. Arun, "Priority Queueing Model-Based IoT Middleware for Load Balancing," 2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS), 2022, pp. 425-430, doi: 10.1109/ICICCS53718.2022.9788218.

[14]. M. Nagabushanam, H. G. Govardhana Reddy & K. Raghavendra (2022) Vector space modelling-based intelligent binary image encryption for secure communication, Journal of Discrete Mathematical Sciences and Cryptography, 25:4, 1157-1171, DOI: 10.1080/09720529.2022.2075090.

[15]. Pankaj Mudholkar, Megha Mudholkar, B S Puneeth Kumar and S. Srinivasulu Raju (2021), Smart Villages: IoT Technology Based Transformation, Journal of Physics: Conference Series, 2070(1), pp. 012128. https://doi.org/10.1088/1742-6596/2070/1/012128.

[16]. Gurung, S., Chauhan, S.: A dynamic threshold based algorithm for improving security and performance of AODV under black-hole attack in MANET. Wireless Networks, 25(4), 1685-1695 (2019).

[17]. Jacob, S.S., Hussain, N., Chennappan, R., Sakhare, D.T. (2023). Convergence of Communication Technologies with Internet of Things. In: Hemanth, J., Pelusi, D., Chen, J.IZ. (eds) Intelligent Cyber Physical Systems and Internet of Things. ICoICI 2022. Engineering Cyber-Physical Systems and Critical Infrastructures, vol 3. Springer, Cham. https://doi.org/10.1007/978-3-031-18497-0_48

[18]. Rajeswari, A.R., Kulothungan, K., Ganapathy, S. and Kannan, A., 2019. A trusted fuzzy based stable and secure routing algorithm for effective communication in mobile adhoc networks. Peer-to-Peer Networking and Applications, 12(5), pp.1076-1096.

[19]. Krishnan, R.S., Julie, E.G., Robinson, Y.H., Kumar, R., Son, L.H., Tuan, T.A. and Long, H.V., 2020. Modified zone based intrusion detection system for security enhancement in mobile ad hoc networks. Wireless Networks, 26(2), pp.1275-1289.

[20]. Bisen, D. and Sharma, S., 2018. An enhanced performance through agent-based secure approach for mobile ad hoc networks. International Journal of Electronics, 105(1), pp.116-136.

[21]. Vatambeti, R., Sanshi, S. and Krishna, D.P., 2021. An efficient clustering approach for optimized path selection and route maintenance in mobile ad hoc networks. Journal of Ambient Intelligence and Humanized Computing, pp.1-15.

[22]. Vatambeti, R., 2020. A novel wolf based trust accumulation approach for preventing the malicious activities in mobile ad hoc network. Wireless Personal Communications, 113(4), pp.2141-2166.

[23]. Xu, H., Si, H., Zhang, H., Zhang, L., Leng, Y., Wang, J. and Li, D., 2020. Trust-based probabilistic broadcast scheme for mobile ad hoc networks. IEEE Access, 8, pp.21380-21392.