Intelligent Automation & Soft Computing
DOI:10.32604/iasc.2021.017547
Article

Tech Science Press

Trust Management-Based Service Recovery and Attack Prevention in MANET

V. Nivedita[1,*] and N. Nandhagopal[2]

[1]Department of CSE, Star Lion College of Engineering and Technology, Thanjavur, India
[2]Department of ECE, Excel Engineering College, Namakkal, India
[*]Corresponding Author: V. Nivedita. Email: nivenivedita1991@gmail.com
Received: 02 February 2021; Accepted: 25 March 2021

Abstract: The mobile ad-hoc network (MANET) output is critically impaired by the versatility and resource constraint of nodes. Node mobility affects connection reliability, and node resource constraints can lead to congestion, which makes the design of a routing MANET protocol with quality of service (QoS) very difficult. An adaptive clustering reputation model (ACRM) method is proposed to improve energy efficiency with a cluster-based framework. The proposed framework is employed to overcome the problems of data protection, privacy, and policy. The proposed ACRM-MRT approach that includes direct and indirect node trust computation is introduced along with the master recovery timer (MRT) for achieving an efficient service recovery process, and its service recovery time is calculated through the service execution process. During data transmission in MANET, various types of attacks can occur, of which the Sybil attack is the most dangerous. To address this problem, this paper proposed a method for the detection and prevention of Sybil attacks using a resilient scheme. The proposed method can improve system energy efficiency and address security, safety, and privacy issues of wireless network applications. Finally, the performance of the proposed method is evaluated regarding the time delay, throughput, energy efficiency, control overhead, and detection rate. The simulation results show that the proposed ACRM-MRT method can effectively improve the time delay, throughput, energy efficiency, control overhead, and detection rate compared to the existing methods. Topological change adaptive ad-hoc on-demand multi-path distance vector (TA-AOMDV)and ad-hoc on-demand multi-path distance vector (AOMDV) are simulated on the NS2 platform for the data rate in the range of 4–40 kbps and the number of nodes in the range of 10-100. The proposed method can reduce the service recovery time in the case of faults during service execution and can be used in real-time applications traffics since it is mostly affected by failure through the occurrence of delay and loss of packets.

Keywords: MANET; routing algorithm; adaptive clustering reputation model; master recovery timer; sybil attack; data protection; privacy and policy

1 Introduction

The mobile ad-hoc networks (MANETs) have been widely applied to various fields, including recovery during a disaster, video conferencing, and emergency treatments, such as battlefield communications with the most likely transmission of audio/video data. The development of the Internet of Things (IoT) has further supported the MANET implementations by using intelligent devices, such as network nodes. However, an enormous demand for multimedia transmission is focused on quality-of-service efficiency (QoS). Today, ensuring the QoS in MANETs is very difficult as it lacks satisfactory management and central node resource planning and is also subjected to external intervention and internal failures, such as link breakage, battery loss, explosions in traffic, heavy traffic, and process failures. Besides, the mobility of nodes unpredictably alters network topology, which in turn affects link stability. By considering the cluster-based routing method, the cluster head that collects data from its member nodes aggregates these data and transmits the collection of data to the receiver using a single-hop or multi-hop routing method. The multi-hop routing method provides a chance for nodes to discover activities of malicious nodes in a MANET. Due to the existence of malicious nodes, secure routing protocols and proper design of mobile sensor nodes are necessary. The malicious nodes can affect data packets intentionally or misguide the messages in the routes or cause the active packets routing to be repeated from the standardized sensor nodes to the trustable neighboring nodes that, after the cluster heads, have the highest trust for efficient ad-hoc routing process. Considering this, the high trust values from the cluster heads to be selected depend on attacking nodes prevention from the cluster head.

Therefore, it is necessary to isolate malicious nodes from various cluster members to reduce illegal activities and avoid tampering activities in a network that can decrease the trust value-based accuracy. The defense methods that have been employed in wired networks are too rigid to be appropriate for MANET having restricted resources and processing power. This work focuses on Sybil attacks because these attacks are the most severe attacks in MANET and can be easily launch in mobile ad-hoc networks where the communication medium is open and broadcast, which can have a serious impact on wireless network performances. A Sybil attacker can mislead other nodes by presenting a duplicate ID or wrong ID of a consumer who is conscious of wireless sensor network (WSN) nodes. Namely, WSN nodes are not organized into a fixed infrastructure, and a WSN consists of multi-hop and single-hop communication, gateways, base station, and access points. Basically, a MANET has a relatively small infrastructure, so it can be considered as a non-infrastructure network. It has been widely employed in industrial wireless networks and applications to address security, safety, and privacy problems. This technique is applicable to solving problems related to data protection, privacy, and policy since it uses a security mechanism against an attacker, so data transmission and communication are safe and secure. The remainder of this paper is organized as follows. The related works are reviewed in Section II. The proposed method is introduced in Section III. The simulation results and discussion are presented in Section IV. Finally, the conclusion and future work directions are given in Section V.

2 Related Works

An energy-efficient ad-hoc on-demand routing (EEAODR) algorithm [1] focuses on conventional ad-hoc on-demand distance vector (AODV) responsibilities to meet specifications, such as organizing hub-based vitality stack for improving system consistency. A discrete Wavelet transform (DWT)-based technique for detecting anomalies in WSNs that can be organized in vital infrastructures, such as energy grids, was presented in Saganowski et al. [2]. An innovative SNORT-based pre-processor was implemented to develop efficient DWT-based anomaly detection technique. The discrete wavelet transform was applied to 26 network traffic parameters considered in the real test bed. Furthermore, this method was implemented as an algorithm in a SNORT pre-processor so as to achieve the performance of the state-of-the-art intrusion

detection systems. The denial-of-service (DoS) is an attack to make a network resources unavailable to its intended users by temporarily disrupting services of host connected to internet [3].

The MANET does not directly relate to the big data, so how to solve the MANET using the big data approaches, such as secure, reliable data collection from MANET and calculating necessary data from the big data sets and transmission was discussed in Biabani et al. [4]. The approaches, such as cryptographic authentication that have four phases, including verification of trust nodes in the IoT environment, node routes testing, discovery of gray hole attack, and elimination of malicious attack in MTISS-IoT, were studied in Mabodi et al. [5]. A novel trust-based energy-aware routing (TEAR) with the degradation of cruel black hole attack (BHA), which satisfies the requirements for security and energy efficiency, and high degradation of numerous security attacks in MANET, was proposed in Merlin et al. [6]. The AODV routing protocol intended for a case of numerous hazardous attacks that could diminish network performance was proposed [7]. A novel intelligent agent-based strategy considering the hello packet table (NIASHPT) to address the problems caused by black hole attacks was proposed in Seyedi et al. [8]. Farhan Ahmad et al. [9] focused on Cloud integrity and privacy mechanisms relying on hardware tamper-proof and cryptographic data structures that were energy-efficient and proved these mechanisms were suitable for untrusted Cloud environments [9]. In Mostafa et al. [10], it was studied how to achieve a better quality of S-box designing and efficient processing time to reject attacks and thus improve secrecy. A cryptography technique based on the security model that helps the AES-based encryption approach to generate secret keys, which are then used to encrypt or decrypt the messages, was proposed in Awan et al. [11].

An approach of providing insight features to a wireless ad-hoc network system from the routing protocol perspective is secure. In Zhou et al. [12], several attacks in MANETs were studies, and security techniques for routing protocols were introduced [12]. Various attacks in a mobile ad-hoc network (MANET), including DoS, user-to-root (U2R) attacks, probe attacks, and vampire attacks, were analyzed in Vaseer et al. [13]. A game theory approach with an energy-efficient network-based routing protocol was proposed to enhance the QoS routing in MANET while improving efficiency [14]. The low energy adaptive clustering hierarchy (LEACH) protocol that matches the group formation and trust values exchanged among the member nodes, master nodes, and Base station was proposed in Ramesh et al. [15]. In a wireless network, mobile nodes collaborate with each other in order to provide the multi-hop communication between the source and destination node. An important assumption in a MANET is that each network node is a trusted node [16]. An approach of intrusion detection-based available network routing for a mobile ad-hoc network, which can decrease both the packet loss rate and the end-to-end delay, was introduced in Sivakumar et al. [17]. An intrusion detection cum trust-based framework for attack detection and network reliability maintenance was proposed [18]. The WSNs have been widely applied in many fields, including environmental monitoring and water quality monitoring. Variety of WSN-based methods for water quality monitoring have been proposed and analyzed regarding their energy, coverage, and security aspects [19]. The WSNs have also been used in many other fields, including industry, health, and military. With a number of intrinsic restrictions in WSNs, a critical concern is security. The stated functions of wireless devices' security must be well established. In Wei et al. [20], a method for security testing that depends on security levels was suggested for WSNs. The experimental results showed that the proposed platform was feasible for the assessment of the WSN devices' security levels. A sensor node establishment approach, which was regarded as a demanding task because of restricted sensor nodes' resources, was presented in Albakri et al. [21]. The polynomial-based distribution schemes of sensor nodes were proposed for providing a trivial resolution for devices that were resource-constrained. Particularly, polynomial-based schemes can assure that a pair-wise key between two sensors in mobile nodes is generated. However, the main shortcoming of a completely polynomial-based approach in WSNs is that they are exposed to sensor confined attacks. In particular, an attacker can co-operate the entire network security through a fixed sensor capturing number. In Albakri et al. [21], a polynomial-based scheme was

implemented with a security feature that was probabilistic and could efficiently decrease the sensor-captured attack security risk while requiring a negligible amount of computation memory and overhead. In Soni et al. [22], a scheme of the WSN localization algorithm was tested for various network security attacks under different performances, such as node mobility, node density, packet size, and temperature, to evaluate the residual energy of WSN nodes. The localization algorithms have been susceptible to attacks of network security.

Countermeasures and attacks linked to security issues. In recent years, the MANET has been one of the most challenging and exciting research domains [23]. Due to the aggressive nature of the exploitation surrounding and constrained wireless medium nature resources, more rigorous security challenges on small sensor devices in WSNs have been put compared to conventional networks, namely, attacks on hardware or software parts can cause severe network damages. Therefore, an efficient and effective security method for preventing these attacks has to be implemented in the system design phase. This approach summarizes the most important WSN security aspects. In a narrative approach for service recovery and service execution, which employs further control communication, the fault point can be acknowledged quickly by neighboring devices, which will then take the responsibility of service recovery [24]. In Chen et al. [25], The Topological change Adaptive *Ad hoc* On-demand Multipath Distance Vector (TA-AOMDV) routing protocol was proposed to address the problems of mobility and resource limitation of nodes in MANET. In Gawas et al. [26], QoS aware weight based on demand Multipath Routing protocol (QMR) was proposed to enhance Quality of Service in routing in MANET. In Chen et al. [27], the routing protocol AOMDV was proposed by considered two criteria route balancing and power conservation based on cross layer design. In Periyasamy et al. [28], Link Reliable Multipath Routing (LRMR) protocol was proposed to address the problems of link failures and route breaks. In Giri et al. [29], Ad-hoc On Demand Multipath Distance Vector (AOMDV) using Teaching-Learning Based Optimization (TLBO) technique was proposed to address certain limitations like road constraint, speed of vehicles in VANET. In Manisha Yadava et al. [30], key appropriation RSA technique was utilized for data security in giving accessibility, and security where the sender and recipient need to guarantee secure transmission of information. In Yong Huang et al. [31], ScatterID, a lightweight system was proposed that attaches feather light and battery less backscatter tags to single-antenna robots for Sybil attack mitigation.

3 Proposed System

This section introduces the proposed system. The secured communication of data is the major concern of the proposed network system so as to provide a protected data communication. Thus, the proposed method is efficient in offering data protection, privacy, and policy.

3.1 System Model

Initially, two general models are presented to give a suggestion regarding the information transferring between mobile nodes. It is assumed that there are N mobile nodes that are moving at a certain distance according to the reference region model of group mobility. All of the nodes in the model have equivalent transmission ranges, and each node is capable of transferring information to its neighboring nodes.

3.2 Node Deployment

Initially, the network initialization is carried out and followed by node deployment. The network deploys each node in the network. The scenario containing two types of non-cooperating users, i.e., secondary users (SUs) and primary users (PU's), is considered. For instance, PUs, which can be cellular phones, wireless microphones, or TVs, denotes users to whom the wireless spectrum amount has been being approved. Conversely, the SUs denote users without pre-assigned wireless spectrum.

The SUs can broadcast their own packets by seizing the time when PUs does not use the certified wireless spectrum. In this, the accessible wireless spectrum of SUs is divided into a number of channels having a predetermined frequency bandwidth. The energy competent-distance vector routing (EC-DSR) has been regarded as an energy-efficient reactive routing protocol that can establish on-demand routes by offering a lower delay at the connection phase. For a new destination, routes can be chosen easily by nodes that have been incorporated in dynamic communication. It supports both multicast and unicast routing types. The shortest routes without loops represent optimal routes for data transferring between mobile nodes. In the proposed EC-DSR protocol, to reach the destination node, the source node sends the route request (RREQ) packets to all its neighbors. The RREQ consists of seven fields: packet lifetime, request ID, source and destination addresses, source and destination serial numbers, and a distinctive identifier. A higher serial number of a node aids in the determination of updated information from the node. This process is continued by the source node till the destination node is found. If the neighbor node is the destination or it knows the path to the destination node, then the route reply (RREP) packet is sent to the source node for the purpose of acknowledgment. The flowchart of the proposed system is shown in Fig. 1.

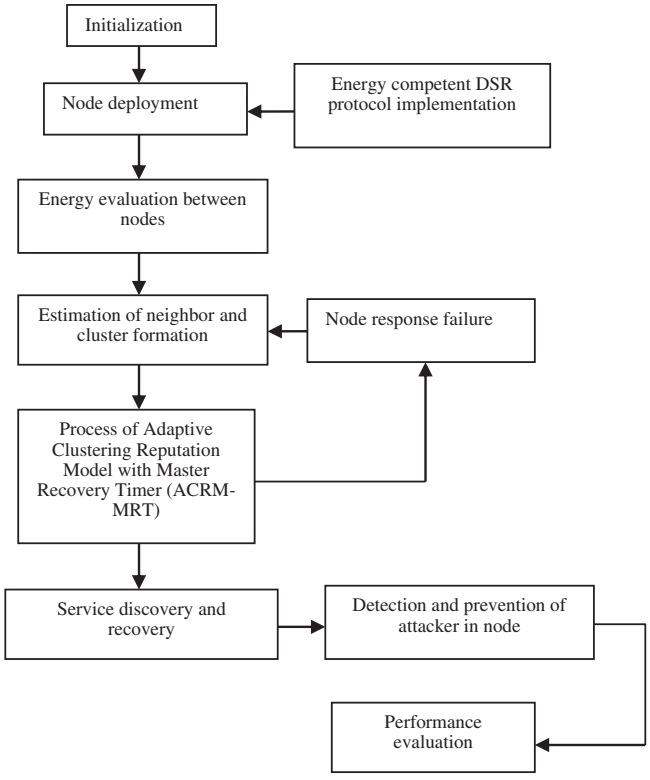

Figure 1: Flowchart of the proposed system

3.3 Energy Evaluation between Nodes

The evaluation of energy trust between nodes starts with the evaluation of node performances. Therefore, the energy factor estimation can be used to avoid effectively nodes' lower aggressiveness in network operation. The node's energy consumption is equal to or greater than the pre-defined energy threshold, E_{Thres}, so as to pursue the life span of the network depending on the node's simple basic function and thus regulate the energy consumption between nodes. The evaluation principles of energy trust between nodes can be expressed as follows:

$$Te_j(t) = \begin{cases} 0, & if\ E_R < E_{Thres} \\ 1, & else \end{cases}, \quad (1)$$

where correspond to $E_{R\ denotes}$ denotes the node's residual energy, $E_{Thres}E_{Thres}$ in turn communicate to represents the energy threshold, and $Te_j(t)$ denotes the average energy trust.

3.4 MANET Clustering

Clustering is employed for a transmission cost reduction and for saving the battery life of a network. It can be regarded as a grouping technique in which, within a group of sensors, only the group head (cluster head) can transmit data. This represents the implementation of a hierarchical network where, in contrast to a flat network, there are a number of valued nodes, which represent higher-level nodes that have a supplementary duty. A similar hierarchical technique is employed in clustering. Cluster heads are at a superior level, and they acquire data sensed by lower-level cluster members. Cluster heads then combine the collected sensory data and forward it to the other cluster heads, which are base station or higher-level nodes. The most important clustering objective is to reduce the power needed for communication so as to save the sensor network's battery life. Clustering protocols can be roughly divided in to distributive and centralized protocols. Some of the clustering protocols are power-dependent, some are location-aware, and a certain number of protocols have features of both multi-level clustering and multi-hop inter-cluster communication. The network nodes are grouped into clusters based on energy clustering. Initially, all of the clustered nodes analyze their neighboring nodes' trust values and choose a Cluster Head (CH) node. To avoid selecting a malicious node, which changes its status often, as a CH, it is essential to choose a CH that is trusted. The selection of CH depends on node weight that consists of many parameters, including trust computation and direct and indirect trust computation. The node with the highest trust value will be selected as a CH. The Clustering structure in MANET is shown in Fig. 2.

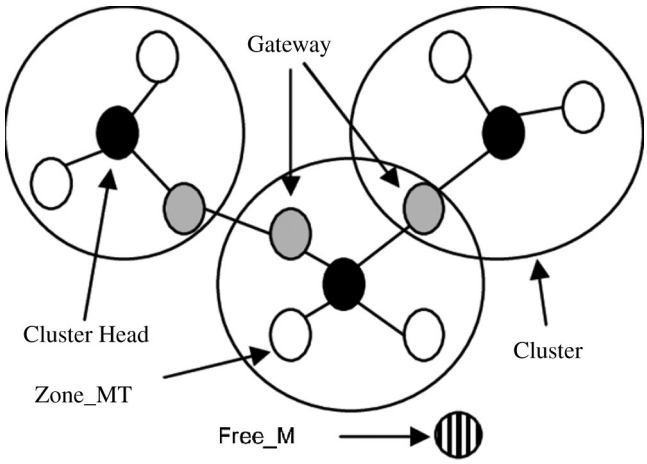

Figure 2: Clustering structure in MANET

3.5 ACRM-MRT

The node trust calculation can be indirect or direct, as explained in the following.

Direct trust calculation - Mobile nodes have implemented mechanisms for computing the trust values of their neighbors. In the direct trust calculation, the behavior of a target node is observed by the source node. The observed data include details of the target node communication. Once all details are collected, the details regarding the total numbers of successful and failed transactions are computed. By means of the direct trust

node calculation, the trust value of the destination is estimated based on which the destination node is evaluated. Thus, the neighboring nodes are monitored through listening to their communication passively, and each network node monitors its neighboring nodes' behaviors. The identification of packet drop, delayed packet, and forwarded packet shows whether the neighbor node drops or forwards data. The monitoring of direct trust reviews the collected data. The agents of direct trust (DT) perform trust calculation. A node X needs to estimate the trust value of a node Y denoted as K of DT as follows:

$$K = S - F, \tag{2}$$

where S denotes a successful communication metric function, F denotes the function of communication metrics that are not successful. By the DT evaluation of Y, X will be provided with subsequent information. Function S relates to forwarded control packets and received control packets, while function F relates to delayed packets and dropped packets. As mentioned above, K represents the DT value of node Y estimated by node X

Hybrid trust calculation – This calculation represents the combination of direct and indirect calculation methods. Each node in a network gets information on the other network nodes. This information is stored in each node and then used in trust value calculation. The energy-based clustering is performed, and the master recovery timer is employed for controlling clustering operation performance.

In this calculation method, the trust calculation is periodically performed to enhance the security level of network nodes after the expiration of each time as follows:

$$T\left(\frac{p}{\partial}, \mu\right) = \left[\frac{\varphi(\partial + \mu)}{\varphi(\partial)\varphi(\mu)}\right] p^{\wedge}(\partial + \mu)^{\wedge}(\mu - 1), \tag{3}$$

Where ∂ denoted the normal behavior of a node, and denotes the μ denotes the abnormal node behavior; T represents the trust value.

In a MANET, how to determine the energy, computational power, bandwidth, and memory of nodes according to the security design components is a demanding task. The hybrid trust value consisted of direct and indirect trust values is expressed as:

$$T_{i,j}(t) = W_1 T^d_{i,j}(t) + W_2 T^r_{i,j}(t), \tag{4}$$

where is "$T^d_{i,j}(t)$ denotes the direct trust value obtained by the direct trust calculation, and $T^r_{i,j}(t)$ is the trust degree that represents the indirect trust value obtained by the indirect trust calculation, which depends on the recommendations of node I (neighboring node) in the direction of node j at time t; W_1 and W_2 are the weights of node i [0,1]that denote a constraint to the individual weight assessment by node I of the direct trust on the route of j node; each trust value has its specific individual values W_1 and W_2; value $T_{i,j}(t)$ represents the average trust degree, that is close to the true status of node j at time t. The trust value update is triggered by encounter events to enhance the security levels of nodes in the network after the expiration of each time. Before each encountered event, node I attains direct observations either in the direction of j (when node I encounters node j) or oblique recommendations to node j (when node i encounters node m, $m \neq j$)

The node trust degree is calculated by;

$$T_{i,j}(t)^l = \alpha_1 PT^d_{i,j}(t)^{l-1} + \alpha_2 NT^r_{i,j}(t)^{l-1} + ids(i,j)^l \tag{5}$$

where $PT^d_{i,j}(t)^{l-1}$ denotes the direct trust value of node j calculated by node I based on the collected information on node j, and $NT^r_{i,j}(t)^{l-1}$represents the indirect trust value of node j calculated by node I based on the previous behavior of malicious node j; $\alpha_1$and denote α_2 denote the exponential factors of negative and positive decay time evaluations, respectively; $ids(i,j)^l$ denote the behavior evaluation of

node j obtained using the intrusion detection system; $T_{i,j}(t)^l d$ denotes the average trust degree; lastly, $ids(i,j)$ is specified by

$$ids(i,j) = \begin{cases} P, \ for \ 0 < P < 1 \\ 0, \ \ for \ uncertain \\ N, \ for -1 < N < 0 \end{cases}, \tag{6}$$

where P and N denote the negative and positive behavior assessments of node j, respectively the positive and negative assessments follows the rule that superior repute is harder to obtain than the bad one. The value of asterisk $(*)$ is set to zero when the node's behavior judgment is not sure; $ids(i,j)$denotes the estimation of the current behavior of node obtained by employing the intrusion detection system. So, to address the on-off attack, decay time adaptive exponential factor α is defined as follows:

$$\alpha = \begin{cases} \alpha_1 = e^{-\rho_1 * (tc-td)}, \ for \ PT_{i,j}^d(t)^{l-1} \\ \alpha_2 = e^{-\rho_2 * (tc-td)}, \ for \ NT_{i,j}^r(t)^{l-1} \end{cases}, \tag{7}$$

where td represents the time, and tc stands for the current time once the last communication happens. In accordance with the above equations, the value of trust decreases with time. When, $\rightarrow 0$, the outcome of the current communication is more significant than that of the previous ones. In Eq. (7), $PT_{i,j}^d(t)^{l-1}$ corresponds to the direct trust value of node j for node I and depends on the previous tractable performance of node j, whereas $NT_{i,j}^r(t)^{l-1}$ is the indirect trust value of node j for node I that depends on the past malicious actions of node j. The weight factors are based on actual circumstances. An on-off attacker can first act well and then gain a reasonably poor elevated reputation. Under this circumstance, a low value of α is set for the well-behaved nodes records and a high value for malicious records. This method reveals that the behavior of a malicious node will be remembered for a longer time compared to that of a well-behaved node. Accordingly, an on-off attacker can hardly obtain a superior reputation because that requires a consistent and long-time well-behaved communication behavior. Then, the direct trust is calculated as:

$$\sum_{(k \in i,j)}^{n} T_{i,j}(t)^l = \sum_{(k \in i,j)}^{n} T_{i,j}^d(t)^l * T_{i,j}^r(t)^l. \tag{8}$$

In this technique, the trust calculation method is employed for estimating the sensor nodes' indirect trust values. In Eq. (8), $T_{i,j}^d(t)^l$ denotes the direct trust value of node j for node i,$T_{i,j}^r(t)^l$ represents the indirect trust value of node j for by node i that provides the data suggestion, and $T_{i,j}(t)^l$denotes the average trust value. In order to handle collusion and bad-mouthing attacks, an inconsistency check scheme is proposed, and it is defined as:

$$ic(i,j)^l = \frac{\sum_{(k \in (i,j)}^{n} T_{i,j}^d(t)^l * T_{i,j}^r(t)^l + T(i,j)^l}{\sum_{(k \in (i,j)}^{n} T_{i,j}^d(t)^l + 1}. \tag{9}$$

As mentioned before, the collected recommendations may include false data provided by collusion attackers and bad-mouthing attackers. For all recommendations, the trust computation model uses a threshold ε to determine whether the information is suspicious. If $\left| T(i,j)^l - ic(i,j)^l \right| > \varepsilon$, the data recommendation is discarded, and in this case, if a malicious node is included in the set of trusted devices and provides false information, this can be detected quickly since false recommendations have different dissimilarity (lower or higher) from the true ones.

3.6 Master Recovery Timer

A fault that is caused by means of the wireless link breakdown in several cases cannot be detected till the timer set by the service originator expires. The execution plan of service backup is not chosen till the process of service discovering is completed. The restarted service execution process includes messages resending those results in redundant data traffic to the network. In addition, the service originator consumes time resources to obtain a response, which cannot be delivered to it, which generates redundant network overhead. The faults of execution service on the Internet can be roughly classified into three types: faults caused by computational logic or the semantic errors, faults caused by the congestion or disconnection of the network in the MANETs that vary greatly from the recovery of service on the Internet, and faults of service execution in the MANETs caused by the network's dynamic topology. The last mentioned fault type is introduced by node mobility in the network, and in dynamic network topology, the strategy of service recovery ought to mostly aspire at dealing with a broken link and searching for alternate services. For the atomic service, a timer is set, but when the factor fails, a replacement is used to restore the previous atomic examination. Each network node stores the information on its list of services and service information gathered from its adjacent nodes. The information transmission service between nodes uses a method similar to the Hello message that is employed in the AODV routing protocol for realizing the connectivity from node to its adjacent nodes. The acknowledged service information of a node is appended to the Hello message and broadcasted to the adjacent nodes in one hop. The same as in the conventional recovery method, a single timer is set using the service originator for monitoring the service execution to determine whether a liability occurs. In the case that the service originator gets a null response from the service provider when the time expires, it is considered that the implementation has been unsuccessful, and the process of service implementation is restarted if essential. However, this method differs from the conventional technique in two aspects, namely, in the conventional technique, the service originator only knows that a liability has occurred on the path of service execution but has no information on the exact fault location. This can lead to the response to the third query since the service originator starts to repair the liability because it has no knowledge about the fault location.

3.7 Service Discovery and Recovery

Service routing is the exchange of information (packets) between nodes. The major goals of routing are not only to discover but also to recover routes in the case of link breakages and malicious nodes between the source and destination nodes in a dynamic network topology using the minimum resources. During the data transmission in a WSN, there is a possibility of various types of attacks. Among these attacks, the Sybil attack is the most severe and the hardest to handle. Therefore, the detection and prevention of the Sybil attack using a resilient scheme are considered in this work. Also, the energy efficiency of the network system is improved. When the service interruption happens, the service requester checks the service list and acknowledges an alternate service provider. When the alternate service provider receives the request message; it executes the service and returns the response to the service requester. When the service requester gets the response from the alternate service provider, it acclaims to the user that the service execution has succeeded, and then performs secure service routing and provides service for the service requester continuously. When a node receives the RREQ packet, wherein the information on the source node is stored, and the node updates/adds the entry to the routing table and creates an RREP message. The RREP packet is then broadcasted to the source node. If the node does not get the RREP in a particular time period, the source node will select the alternate service provider from the service list, thus maintaining and executing the service between the source and destination. Scheduling is one of the most critical aspects of cellular networks; it decides which relations should be transmitted where and at what speed of data.

3.8 Detection and Prevention of Attack Using Resilient Scheme

In the EC-DSR routing protocol, the main objective is to prevent and identify a Sybil attack, which is performed by the projected method that is based on the identity verification approach. The proposed method

uses the EC-DSR algorithm and the intrusion detection scheme for the prevention and detection of a Sybil attack. Also, the resilient approach is introduced for the detection and prevention of a Sybil node. First, it is necessary to distinguish an authenticate node from a Sybil node. The implemented algorithm can easily compute the trusted values of network nodes. By a majority vote of neighbors, a node is classified into a certain class. The resilient scheme generates a collection of randomly selected decision-making zones. This combines votes of several decisions depending on the normal and abnormal features, the correlation between the packet lost and nodes normal and abnormal features. To calculate the trusted value, the correlation needs to be calculated first, and it is calculated by:

$$Correlation\ (i,j) = \sqrt{(A_{n_{fea}}(i,1) - A_{n_{fea}}(j-1)) + (A_{n_{fea}}(i,1) - (A_{n_{fea}}(j,1)^2}, \tag{10}$$

where $A_{n_{fea}}$ represents the abnormal nodal features, and I and j are correlation coefficients.

As we conditioned the prototypes on normal node behavior and its features. Here, the node features can be calculated by using Eq. (11)

$$= \ \left[\right] A_{n\_fea} = \left[A_{n\_fea}\text{Distance}\right], \tag{11}$$

Hence the suggested A_{n_fea} denotes the abnormal features of a node.

The proposed resilient scheme can evaluate the features of nodes and can distinguish an authentic node from a Sybil node. The abnormal value of the Sybil node is calculated by:

$$= \ ()A_{SNv} = \ \left(A_{n\_fea}\ dist\right), \tag{12}$$

where A_{n_fea} represents the abnormal value of the Sybil node, A_{SNv} represents the trusted value of the Sybil node based on which the trusted value of the Sybil node can be identified. Therefore, the proposed framework is capable of offering preserved and protected data communication in the network.

4 Simulation Verification

The main objective is to find a short delay channel and deliver an information packet in one attempt to the target. Therefore, the overall performance of the proposed approach was evaluated based on these criteria.

Simulation parameters

The simulation parameters are given in Tab. 1.

Table 1: Simulation parameters

Parameter	Meaning	Value
Area	Rectangular Field	1500 X 1500 m^2
N	Number of Nodes	100
S	Max Mobile Speed	30 m/s
R	Transmission Radius	300m
P	Data payload Size	500 bytes/pac
W1	Weighting factor $T_{ij}d(t)$	0.8
W2	Weighting Factor $T_{ij}r(t)$	0.6
Δt	Time interval of trust update	0.3 s
T	Simulation Time	700 s
M	Number of Malicious Nodes	1–20
γ	Threshold of Trust Degree Value	0.8

Performance Analysis

The performance and feasibility of the proposed approach were evaluated and compared with those of the existing methods [25–29] regarding the following measurement criteria.

(i) Packet delivery ratio: This ratio denoted the ratio of the number of received packets over the number of forwarded packets:

$$P = (Pr/Ps) * 100, \tag{13}$$

where P denoted the packer transmission ratio, P_r is the number of received packets, and P_s the number of forwarded packets.

(ii) Control overhead: This is the ratio of the number of packets received by destination node to the observation time duration.

(iii) Average end-to-end delay: This delay denoted the ratio of the difference between the packet transmission time and the overall time consumption over the overall time consumption and it was calculated by:

$$AD = (Ps - Pr) \ / \ Pr, \tag{14}$$

where P_s denoted the packet transmission time, AD denoted the average delay, and P_r was the overall time consumption.

(iv) Throughput: The throughput denoted the volume of successfully transmitted data in the communication cycle, and it was calculated by:

$$Throughput = (Received\ packet\ number * Packet\ size)/Simulation\ time. \tag{15}$$

In the simulation experiment, the NS-2 simulator system was employed to compare the effectiveness of the ACRM-MRT method with those of the existing routing protocols, the topological change adaptive ad-hoc on-demand multi-path distance vector (TA-AOMDV) and the adaptive ad-hoc on-demand multi-path distance vector(AOMDV). The simulation environment and parameter settings were as follows. The node number was in the range of 10–100, and nodes were distributed in the rectangular area with a size of 1000 m × 1000 m, following a random way mobility model. The max speed of the node was from 2 m/s to 20 m/s, and the maximal transmission radius of all nodes was 300 m. The EC-DSR routing protocol was used. It was supposed that all the nodes were divided into clusters and that the number of clusters was 10. Each cluster contained 10 nodes.

The simulation results regarding different metrics are presented in Figs. 3–6. A shown in Fig. 3, for the same number of nodes, compared to the existing routing techniques, the proposed routing protocol had lower routing overhead. The routing overhead of the proposed ACRM-MRT method was low compared to the routing overhead of the existing routing protocols TA-AOMDV and AOMDV. The proposed routing protocol could recognize the link breakage and find the shortest path, so the message could be sent after the fault occurred; thus, the control overhead was reduced gradually.

The results in Fig. 4 show that the delivery ratios of the TA-AOMDV and AOMDV dropped noticeably compared to the delivery ratio of the proposed ACRM-MRT method. The ACRM-MRT method showed improvement in the packet delivery ratio compared to TA-AOMDV and AOMDV, and the packet transmission efficiency of the proposed protocol was better. The proposed routing technique could identify congestion within a small period of time and could easily identify the shortest route. The proposed protocol could easily sense the link breaks during the route recovery process prior to data transfer so that the data loss was gradually decreased and the packet delivery rate was significantly improved.

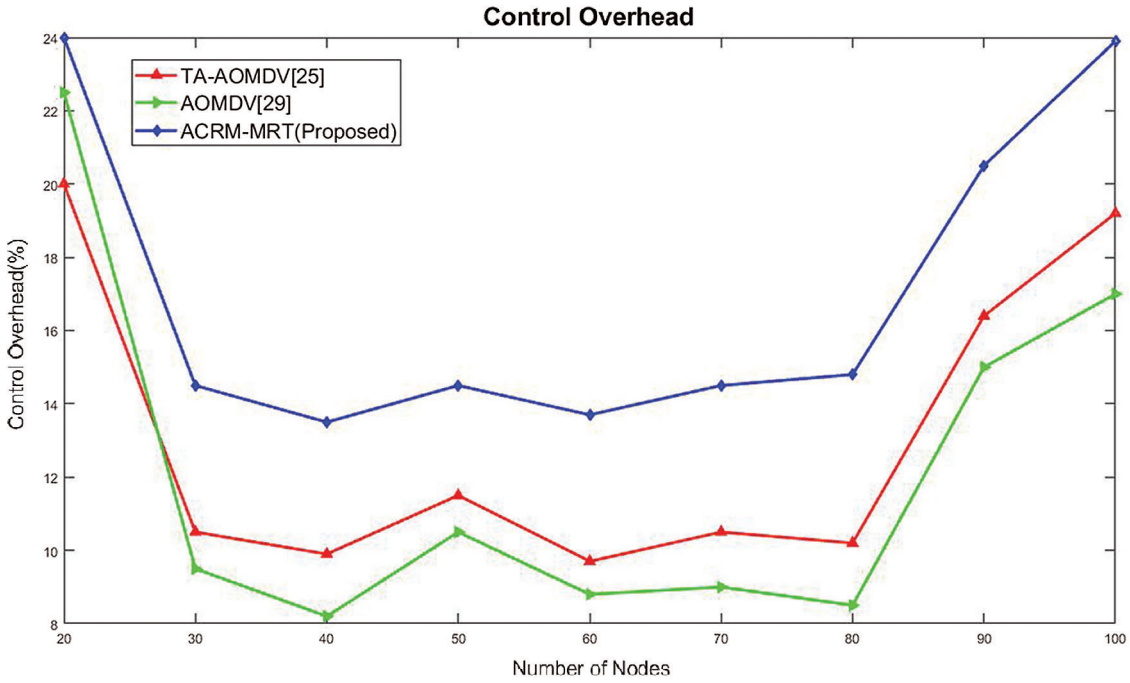

Figure 3: Number of nodes *vs*. control overhead

Figure 4: Number of nodes *vs*. PDR

As displayed in Fig. 5, the end-to-end delay of the proposed protocol was shorter than those of the other protocols. Therefore, the proposed routing technique prevented overcrowding.

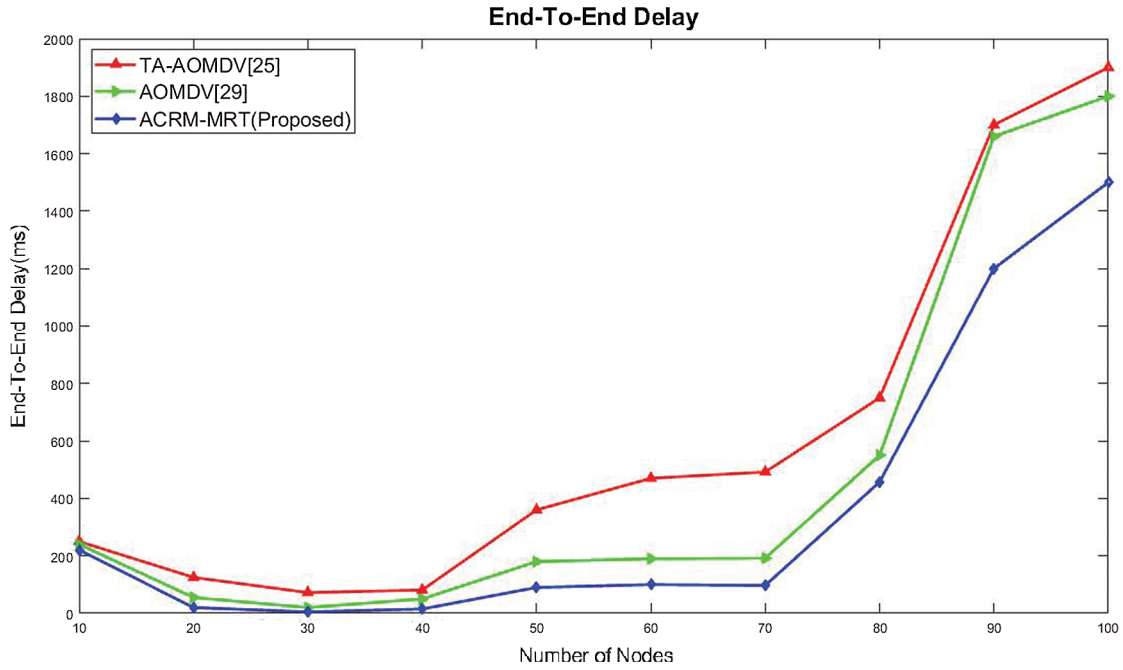

Figure 5: Number of nodes *vs*. average end to end delay

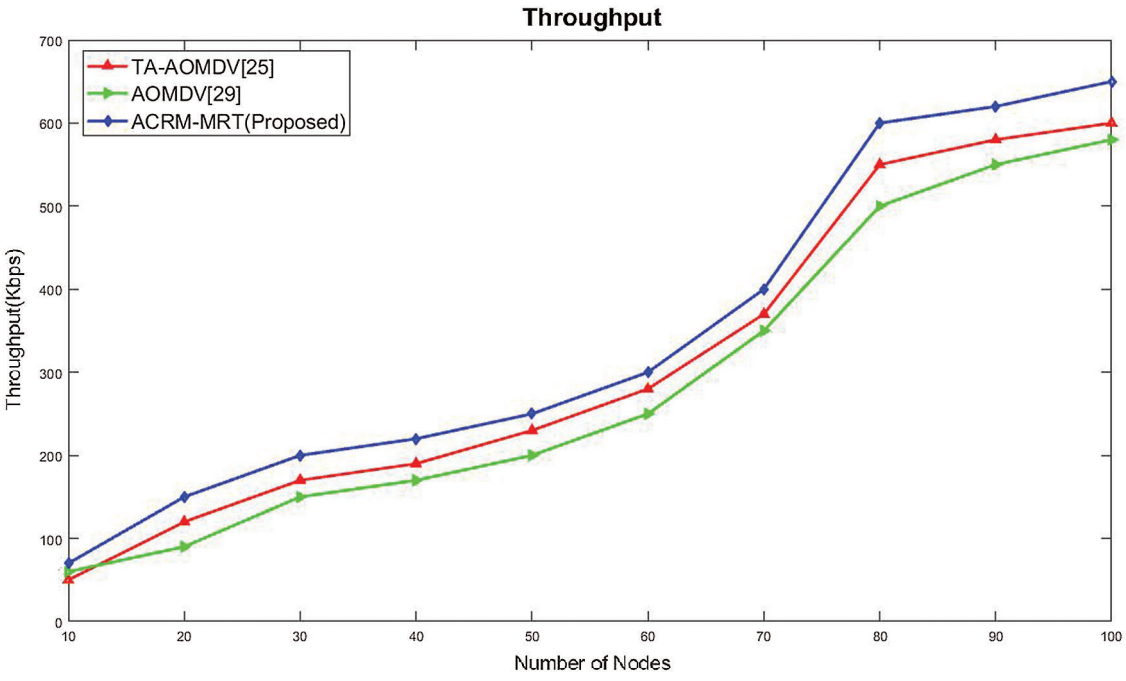

Figure 6: No of nodes *vs*. Throughput

Due to the complexity of dynamic topology in a mobile ad-hoc network, a large number of nodes contributed to the difference in the dissemination of information. Therefore, even when the link was broken, the data could be returned to the source, the new route could be determined, and the cycle could be recovered. It should be noted that in the proposed routing technique, information on the shortest route

and link breakdown was obtained before the loop began. Therefore, the time difference was removed. The end-to-end delay of the ACRM-MRT showed improvement compared to the existing routing protocols TA-AOMDV and AOMDV. The ACRM-MRT had lower end-to-end delay than the TA-AOMDV and AOMDV. The throughput rate comparison results are presented in Fig. 6, where it can be seen that compared to the other routing protocols, the proposed routing protocol achieved a higher throughput rate. When the proposed protocol was used, the shortest path was identified quickly and before the data passed through the route. The throughput rate of the ACRM-MRT was higher than those of the existing routing protocols TA-AOMDV and AOMDV.

The energy consumption comparison is displayed in Fig. 7. The results presented in Fig. 7 reveals that the energy consumption of the proposed protocol was lower than those of the other protocols. Thus, the proposed technique performed better than other comparison techniques in terms of energy efficiency. The average energy consumption of the ACRM-MRT was improved compared to the existing routing protocols TA-AOMDV and AOMDV.

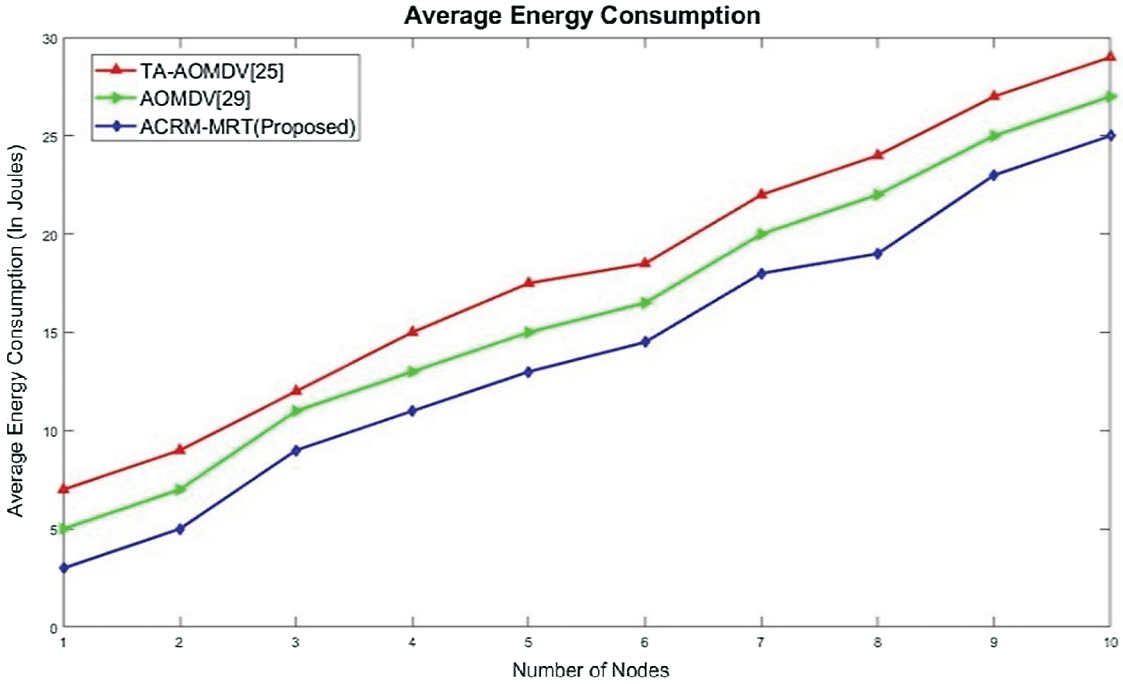

Figure 7: Energy consumption

5 Conclusion and Future work

In the MANETs, the recognition of the Sybil attacks is still a challenging task. To address this challenge, this paper proposes a method against Sybil attacks, which is based on an efficient energy framework. Also, an adaptive link reputation model with trust management of energy optimization in a clustered network is introduced. The ACRM-MRT method that includes both direct and indirect node trust computation methods is proposed for an efficient recovery, and the corresponding service recovery time is computed by the service execution process. In this way, an effective defense against the Sybil attacks is achieved. The localization structure of the Sybil attack, implemented in the trusted protocol, has superior capability in detecting and predicting Sybil attacks. The master recovery timer is employed for controlling the function of node response, which enhances the efficiency of cluster head function. The proposed

technique's performance is estimated by the simulations. The simulation results show that the proposed technique is secured and can protect data transmission and communication in the network system, so it provides an efficient scheme against attacks in MANETs. The results also demonstrate that the proposed technique is highly efficient in the case of Sybil attacks and can recognize the shortest path. Our future work will consider multimedia applications and study how to enhance user experience and offer service in a timely manner in the case of service failures. We will try to detect the specific location of a fault occurring in the network by setting the timers on all intermediate nodes on the path of service execution to offer timely service and enhance the service execution rate of multimedia applications.

Acknowledgement: We thank LetPub (www.letpub.com) for its linguistic assistance during the preparation of this manuscript.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] S. Kalaivanan, "Quality of service (QoS) and priority aware models for energy efficient and demand routing procedure in mobile ad hoc networks," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 3, pp. 4019–4026, 2021.

[2] L. Saganowski, T. Andrysiak, R. Kozik and M. Choras, "DWT-based anomaly detection method for cyber security of wireless sensor networks," *Security and Communication Networks*, vol. 9, no. 15, pp. 2911–2922, 2016.

[3] S. K. Govindan and N. Prasant Mohapatra, "Trust computation and trust dynamics in mobile adhoc networks," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 2, pp. 279–298, 2012.

[4] M. Biabani, H. Fotouhi and N. Yazdani, "An energy-efficient evolutionary clustering technique for disaster management in iot networks," *Sensors*, vol. 20, no. 9, pp. 2647, 2020.

[5] K. Mabodi, M. Yusefi, S. Zandiyan, L. Irankhah and R. Fotohi, "Multi-level trust-based intelligence schema for securing of internet of things (IoT) against security threats using cryptographic authentication," *Journal of Supercomputing*, vol. 76, no. 6, pp. 7081–7106, 2020.

[6] R. T. Merlin and R. Ravi, "Novel trust based energy aware routing mechanism for mitigation of black hole attacks in MANET," *Wireless Personal Communications*, vol. 104, no. 4, pp. 1599–1636, 2019.

[7] A. M. Desai and R. H. Jhaveri, "Secure routing in mobile adhoc networks: A predictive approach," *International Journal of Information Technology*, vol. 11, no. 2, pp. 345–356, 2019.

[8] B. Seyedi and R. Fotohi, "NIASHPT: A novel intelligent agent-based strategy using hello packet table (HPT) function for trust Internet of Things," *Journal of Supercomputing*, vol. 76, no. 9, pp. 6917–6940, 2020.

[9] W. Farhan Ahmad, A. Fatih Kurugollu and A. Sakir Sezer, "NOTRINO: A novel hybrid trust management scheme for internet of vehicles," *IEEE Transactions on Vehicular Technology*, vol. 99, pp. 1–11, 2021.

[10] S. M. Mostafa, I. M. Darwish and M. R. Saadi, "Improved lightweight security approach routing protocol in internet of things," *Internet of Things*, vol. 11, no. 100208, pp. 1–14, 2020.

[11] K. A. Awan, I. Ud Din, A. Almogren, M. Guizani and S. Khan, "Stabtrust—A stable and centralized trust-based clustering mechanism for iot enabled vehicular ad-hoc networks," *IEEE Access*, vol. 8, pp. 21159–21177, 2020.

[12] J. Zhou and Z. Wang, "Security clustering algorithm based on integrated trust value for unmanned aerial vehicles," *KSII Transactions on Internet and Information Systems*, vol. 14, no. 4, pp. 1773–1795, 2020.

[13] G. Vaseer, G. Ghai and D. Ghai, "Novel intrusion detection and prevention for mobile ad hoc networks: A single- and multiattack case study," *IEEE Consumer Electronics Magazine*, vol. 8, no. 3, pp. 35–39, 2019.

[14] P. T. Selvi and C. S. GhanaDhas, "A novel algorithm for enhancement of energy efficient zone based routing protocol for MANET," *Mobile Networks and Applications*, vol. 24, no. 2, pp. 307–317, 2019.

[15] S. Ramesh and C. Yaashuwanth, "Enhanced approach using trust based decision making for secured wireless streaming video sensor networks," *Multimedia Tools and Applications*, vol. 79, no. 15-16, pp. 10157–10176, 2020.

[16] S. Gurung and S. Chauhan, "A survey of black-hole attack mitigation techniques in MANET: Merits, drawbacks, and suitability," *Wireless Networks*, vol. 26, no. 3, pp. 1981–2011, 2020.

[17] S. Sivakumar and P. Vivekanandan, "Efficient fault-tolerant routing in iot wireless sensor networks based on path graph flow modeling with marchenko-pastur distribution (EFT-PMD)," *Wireless Networks*, vol. 26, no. 6, pp. 4543–4555, 2020.

[18] N. Dharini, N. Duraipandian and J. Katiravan, "ELPC-trust framework for wireless sensor networks," *Wireless Personal Communications*, vol. 113, no. 4, pp. 1709–1742, 2020.

[19] M. Pule, A. Yahya and J. Chuma, "Wireless sensor networks: A survey on monitoring water quality," *Journal of applied research and technology*, vol. 15, no. 6, pp. 562–570, 2017.

[20] M. Wei and K. Kim, "An automatic test platform to verify the security functions for secure WIA-PA wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 12, no. 11, pp. 1–12, 2016.

[21] A. Albakri, L. Harn and S. Song, "Hierarchical key management scheme with probabilistic security in a wireless sensor network (WSN)," *Security and Communication Networks*, vol. 2019, no. 4, pp. 1–11, 2019.

[22] S. Soni and M. Shrivastava, "Impact of various networks security attacks on wireless sensor localization algorithms based upon wsn node's residual energy," in *Proc. Int. Conf. on Recent Advancement on Computer and Communication*, pp. 1–10, 2018.

[23] K. Chelli, "Security issues in wireless sensor networks: Attacks and countermeasures," in *proc. World Congress on Engineering*, London, UK, pp. 1–6, 2015.

[24] X. Zhou, Y. Ge, X. Chen, Y. Jing and W. Sun, "A distributed cache based reliable service execution and recovery approach in MANETs," in *Proc. IEEE Asia-Pacific Services Computing Conf.*, Jeju, Korea (South), pp. 298–305, 2011.

[25] Z. Chen, W. Zhou, S. Wu and L. Cheng, "An adaptive on-demand multipath routing protocol with qos support for high-speed MANET," *IEEE Access*, vol. 8, pp. 44760–44773, 2020.

[26] M. A. Gawas, K. Modi, P. Hurkat and L. J. Gudino, "QoS based multipath routing in MANET: A cross layer approach," in *Proc. Int. Conf. on Communication and Signal Processing (ICCSP)*, Chennai, India, pp. 1806–1812, 2017.

[27] J. Chen, Z. Li, J. Liu and Y. Kuo, "QoS multipath routing protocol based on cross layer design for ad hoc networks," in *proc. Int. Conf. on Internet Computing and Information Services, Hong Kong*, pp. 261–264, 2011.

[28] P. Periyasamy and E. Karthikeyan, "Link reliable multipath routing protocol for mobile ad hoc networks," in *proc. Int. Conf. on Circuits, Power and Computing Technologies (ICCPCT–2015)*, Nagercoil, India, pp. 1–7, 2015.

[29] A. Giri, D. Lobiyal and C. Katti, "Optimization of value of parameters in Ad-hoc on demand multipath distance vector routing using magnetic optimization algorithm," *International Journal of Computer Network and Information Security*, vol. 7, no. 12, pp. 19–27, 2015.

[30] P. Manisha Yadava, D. Ajay Shekhar Pandey and A. Karan Singh, "Secure and efficient wireless multicast communication using trust based key management," *Journal of Discrete Mathematical Scieneces and Cryptography*, vol. 9, no 13, pp. 1–17, 2021.

[31] Y. Yong Huang, J. Wei Wang and Z. Tao Jiang, "Detecting colluding sybil attackers in robotic networks using backscatters," *IEEE Transactions on Networking,* vol. 29, no. 2, pp. 793–804, 2021.