Performance Evaluation of BDAG Aided Blockchain Technology in Clustered Mobile Ad-Hoc Network for Secure Data Transmission

B. Harikrishnan[1]*, T. Balasubaramanian[2]*
PG & Research Department of Computer Science & Applications
Sri Vidya Mandir Arts & Science College (Autonomous), Katteri – 636 902, Uthangarai, Tamil Nadu, India[1, 2]
Department of Computer Science, Periyar University, Salem – 636 011, Tamil Nadu, India[1]

***Abstract*—In mobile ad-hoc network (MANET) environment, routing of data packets is a challenging task due to rapid changes in mobility and network topology. In addition, the security aspect of routing is disturbed by attacks caused by malicious nodes. These attacks greatly affect the Quality of Service. To overcome the challenges faced in routing message packets, the Bayesian Directed Acyclic Graph (B DAG) Aided Blockchain model is proposed for clustered MANET environment. The proposed model encompasses the following processes: (i) Multi factor authentication of users by using BLISS algorithm. This step involves acquisition of user credentials and generates hash values for those credentials using Cube Hash algorithm. These hash values are further used to generate public and private keys by BLISS algorithm, (ii) Weighted sum computation for clustering to reduce complexity in the MANET environment. Cluster head (CH) and cluster member (CM) are classified based on energy status, geometric distance, link quality and direction, (iii) A secure AODV based routing protocol using Dolphin Swarm Optimization (DSO) algorithm. This step involves selection of reputed node based on link stability, relative velocity, available bandwidth, energy, queue length, and trust. The packet forwarding is based on the reputation value of the node, by which the trust provided by malicious nodes are eliminated to improve security and (iv) Bayesian DAG aided blockchain, in which the user authenticity, data integrity of packets and signature are verified to mitigate the routing attacks created by nodes in the MANET environment. The proposed model is experimented in NS 3.26 network simulator tool and its performance in terms of multiple QoS metrics is evaluated.**

Keywords—Mobile ad-hoc network; node authentication; BLISS algorithm; blockchain; Bayesian direct acyclic graph

I. Introduction

The current mobile nodes highly necessitate the secure communication. The key goal of this secure communication is to facilitate Quality of Service (QoS) and reliable data transmission in mobile ad-hoc network (MANET) [1,2]. The secure communication in MANET can be established by the combination of trusted mobile nodes and trusted third party. In secure environment, trusted third party plays a crucial role in several disaster applications. The security far-sightedness requirement in MANET is essential because of the succeeding issues, such as vulnerable entities in MANET to the routing attacks (black hole, gray hole, timing and intruder attacks), false warnings in the network and false registered credentials with the transmitted message [4-6] [9]. These issues exemplify the importance of the security in the MANET security. Further, the QoS parameters are affected due to lack of security, stability, and scalability [3]. When the network meets these three factors, each mobile node can be obtained with high QoS by means of high packet delivery ratio, throughput and low packet loss, routing overhead, route acquisition delay, end-to-end delay, and energy consumption.

Authentication is a main process in MANET security that verifies the provided credentials during registration process [6]. Few works [1,2,7] have performed authentication with an aid of blockchain technology to overcome failure during centralized administration when group of attackers combined to target it. Here, the transactions/blocks signature process is performed to provide security in MANET. The public key infrastructure (PKI) based authentication process has performed in blockchain where the Elliptic Curve Digital Signature Algorithm is used to generate key for the data transmission [7,8,15]. In blockchain, elliptic cryptography based authentication is contributed in the MANET. It performs authentication by considering the identity based signature procedures. Routing plays a vital role in the mobile communication and hence, providing security is significant while selecting best next hop. To ensure this, trust based node selection procedures are emerged in the MANET network [10]. In general, source node considers the two trusts viz. direct and indirect trusts for next hop selection [11]. Two different algorithms have utilized for estimation of direct and indirect trusts [12]. In direct trust, recommendation trust is estimated by considering the dropped and forwarded counts of the nodes. The trust is estimated based on two factors that are reputation information collection and trust value estimation procedures. A secure and efficient routing protocol (AOMDV) is designed to provide secure routing in the mobile ad-hoc network [13,14]. The MANET is largely utilized in several sensitive and non-sensitive applications. However, proving security in the MANET is difficult because of the issues, such as dynamic topology, communication latency, network scalability, and high processing security algorithms [16]. These issues induce difficulties in proving security to the MANET. Hence, the main aim and scope of this work is to provide high level security to the MANET network with better data transmission.

*Corresponding Author.

Paper outline: The remaining part of the paper is structured as follows: Section II describes the related works in the field of MANET, Section III presents the major problem statements, Section IV briefly explains the proposed system design and architecture in a well-organized manner and section V presents the experimental settings for the proposed system design and also evaluates the comparison between the proposed as well as previous approaches. Finally, the conclusion is work prospects are presented and summarized in Section VI.

II. Related Work

In this section, the existing works of secure cluster based routing in MANET are discussed. In [17], topological change adaptive ad-hoc on demand multipath distance vector routing protocol (TA-AOMDV) is proposed. This protocol is highly adaptable for high speed node movement in support of QoS. In this protocol, shortest path selection is implemented which takes four parameters as inputs for routing i.e. residual energy, available bandwidth, queue length, and link stability. In general, the path selection is not always optimum due to nodes movement and thus stable path is selected for routing. It considers both path stability and node density, but does not adapt for high speed scenario under large scale environment. In [18], routing attacks (black hole and gray hole) are detected by proposing an intrusion detection system on mobile ad-hoc environment. In attack scenario, the malicious node does not cooperate with other mobile nodes and intentionally disturb data communication by sending false route request & response forwarding and also false data transmission. These behaviors are timely detected in this work through deployment of IDS in most legitimate node. This legitimate node is determined by the connected dominating set model, which considers node energy and blacklist status for deploying IDS entity into it. The proposed method connected dominating set can be applied for small scale region, which is not efficient in large scale region. Further, the IDS deployment is a crucial process that must be running in decentralized mode, since malicious nodes can change the blacklist and nodes energy status. So, the routing attackers cannot be eliminated.

In [19], authors presented graph structure for mobile nodes communication over the network environment. To consume less energy and ensure QoS while transmitting packets from the source to destination node, the graph kernel structure based clustering algorithm is proposed in this work. In graph kernel, all mobile nodes are connected and CH is elected by means of certain significant parameters for data transmission. In particular, there are two processes are executed including cluster head election phase and cluster head maintenance phase. Based on node stability, CH is selected and CH maintenance is initiated by solving K-hop problem and node's current situation (stability and connectivity to other nodes). Among the set of CHs, shortest path is selected. Graph theory consumes more energy where clustering alone can able to perform. Since more computations are required to select K-hop shortest path selection. In [20], a hybrid optimization is proposed for energy related parameters adjustment. As a result of topology changes in network, energy consumption and packet losses during packet transmission is more. To address this issue, chronological and earth worm optimization algorithms are combined as a hybrid algorithm. Clustering is built by graph model (Gabriel graph) where node's power, connectivity, mobility, link lifetime and distance are considered for CH elected. In the graph structured cluster model, data packets having high power and energy are transmitted through nodes. Due to lack of infrastructure, secure communication is the way to minimize errors and data loss for data transmission. This further optimizes power and energy parameters when topology changes exponentially. In [21], network topology is controlled by hybrid artificial swarm intelligence algorithms i.e., robotic Darwin particle swarm optimization with graph based algorithm (RDPSO-GBA). Obviously, transmission delay happens when number of hop counts increases. In graph constructed framework, node's mobility and link connectivity between nodes are predicted. With these criterions, optimal route is selected and routing problem is solved via optimization solution. For route selection, ant colony optimization (ACO) is proposed. However, packet drop rate and energy consumption rate are high. In [22], expected transmission count (ETX) metric is used as one of the metrics to evaluate routing overhead. Through this metric, light ETX, light reverse ETX, and power light reverse ETX that minimizes routing overhead and also improves other ad-hoc network performances. All three metrics are computed for AODV routing protocol and implemented using NS3 network simulator. In experiments, Throughput, Packet Delivery Ratio, Useful Traffic Ratio, Jitter and End-To-End Delay are evaluated. Eventually, ETX does not support for optimum routing because AODV protocol works well in other networks i.e., static network, but does not suit for dynamic networks like MANET.

In [23], author discusses the trusted environment for IoT assisted MANET. The presented trust scheme is a combination of two individual metric i.e., direct and indirect trusts. The sum of direct and indirect trust values is used for final trust value. To compute trust values, beta probabilistic distribution is applied for combining different trust evidences and compute direct trust is calculated. A recommendation trust is computed using ARMA/GARCH, which is predicted for ensuring reliable and secure end-to-end forwarding of packets. Trustworthy nodes are selected in the routing. In [24], author proposes QASEC security routing protocol for secure data communication in MANET. This is a simple and lightweight model for best link selection from the set of available links for packets transmission between nodes. This link must be of optimal transmission link and thus produces minimized end to end delay. To ensure node authenticity, a simple authentication scheme is proposed, which relies on symmetric encryption for each mobile device shared secret keys generation. In particular, device identity, unique session key, and authentication token are considered for legitimate nodes identification. The symmetric encryption requires high energy consumption and also large key size that led to high processing time.

In [25], authors proposed a model for smart packet forwarding based on game theory. This model was proposed to identify and eliminate self-centered nodes which tend to drop the packets thereby increase the retransmission rate and reduce the performance. This model identifies the malicious nodes by considering two factors namely possibility of packet drop and reward factor. Once the node is identified as malicious, the model stimulates the nodes to cooperate in packet forwarding paradigm. The formulated game theory model controls the energy consumption during modulation and data transmission. Even though the proposed method reduces retransmission rate, the network burden and complexity of the method is increased when the number of nodes are increased. In [26], authors proposed a method to protect the packet drop by two major attacks namely black hole attack and grey hole attack. The proposed method uses Artificial Bee Colony optimization algorithm (ABC) based on intelligent swarm algorithm in Artificial Neural Network (ANN) as a deep learning algorithm. The ABC optimization segregates the normal node and attacker node based on the fitness value. The ANN is trained with the output of optimization algorithm and is used to identify the malicious nodes thereby reducing the energy consumption and increasing the security. The ANN used in this method has no determined proper structure; the appropriate structure of the network is achieved through experience and trial and error. The duration of ANN is unknown and this will affect the performance of the method. In [27], authors proposed a model to evaluate the credibility of the mobile nodes by using trust reasoning model based on cloud model and Fuzzy Petri Net (FPN). The routes with minimal trust are selected and added to the routing table. Finally, a routing algorithm based on trust entropy routing algorithm and optimized link state routing protocol is presented. Based on the output of the proposed algorithm, the trust value gets assigned to the nodes and the route selection is carried out on the trustworthy nodes. Fuzzy logic is not always accurate hence results are obtained based on assumptions and the number of rules in the fuzzy logic makes it time consuming. In [28], authors proposed a routing mechanism named Energy Efficient Cloud-Assisted Routing (EECRM), which consists of three phases that cloud assist routing mechanism for efficient employment of route discovery, energy consumption phase for efficient utilization of energy and cloud service update phase. Suppose if any packet drop occurs in data transmission the adjacent route for better transmission is selected and the routing is performed to reduce the energy consumption. The parameters considered for selecting the backup nodes are not sufficient for optimal data transmission. The proposed method does not address problems caused by network attacks but practically these attacks increase latency and reduces performance during data transmission.

III. Problem Statement

This section summarizes the specific problems on blockchain aids and secures routing protocol for MANET. A framework for secure data transmission was proposed in [29]. The blockchain for security data collection in mobile ad-hoc network (B4SDC) framework exterminates of two types of attacks, such as collusion and spoofing. With the use of cooperative receipt report, the collusion attack is detected via control information forwarding for selected routes nodes only and mitigated whereas, the secure digital signature is used for spoofing attacks detection via signing sent messages from source to the destination. Further, excessive message forwarding attack is mitigated through the spoofing attacker's detection. The problem existing in this work, such as blockchain structure is not scalable. As the mobile nodes are always moving dynamically throughout the network, the use of conventional blockchain chain structure is not suitable.

Transaction confirmation time is higher since ECDSA, and $(SHA\text{-}2)^2)$ consumes more processing time. Furthermore, creating blocks for dense MANET consumes high energy compared to clustered environment. Authentication is implemented and security credentials are transmitted through public channel and secret keys are received by the same that may facilitate the receiving of key by the compromised and malicious nodes. The mining complexity is higher for verification of block transactions during message transmission. Hence, a secure routing protocol was proposed to defend against the popular network attack named black hole attack [30]. This work is called as Blackhole Protected AODV routing protocol (BP-AODV) for malicious nodes detection. In routing process, blackhole attackers are detected through nodes past behaviors. Here, the history of node is collected and stored in routing table. To ensure security in the routing process, Chaotic Map features (Ergodicity, Randomness, and Sensitivity) are added which control the conditions and control parameters. However, the above work contains the following significant problems: Chaotic Map is not efficient enough because it needs successive monitoring neighbors' nodes. Besides, it also consumes more bandwidth during data transmission. Further, challenge at source node and secret responses at destination node are not be optimal when nodes move at high mobility. The routing is performed through BP-AODV protocol, which is not efficient to find optimum route since trustworthiness of nodes are computed by historical behaviors. This requires more packet retransmission due to poor computations of trust. Thus, it causes high packet losses and requires optimized solution. To evaluate the trust of the node, a support vector regression based corrective linear program classification model was proposed [31]. The main aim of this work is to reduce minimum end to end delay and maximize packet delivery ratio. In the first step, Tanimoto kernelled support vector regression is proposed to predict node features, such as node history and current energy status. Based on the node examined information, nodes are classified into two classes as "Trusted & Non-Trusted Nodes".

Subsequently, linear program boost classifier is used for trusted node selection for secure data transmission. Here, routing is performed based on node history, current energy status, and cooperativeness. In MANET environment, mobility of the node is more important, since lack of mobility information leads to high data loss. Further, trust values can be easily modified by malicious users. Tanimoto kernel in SVM provides less accuracy in trusted node prediction so that packet losses by malicious nodes involvement and also it leads to poor accuracy when mobile nodes mobility at high rate. To improve the energy efficiency and reduce complexity clustering based protocol was proposed [32].

The fuzzy logic based clustering is presented for cluster formation and cluster head selection. The cluster heads are selected by energy status, node degree, distance, trust level, and node mobility. A standby CH is also presented in case of

CH dies, moving out of coverage, or CH comprises. After the CH selection, trusted nodes are determined for secure route determination. Nevertheless, 243 fuzzy rules are generated for CH election, which increases energy consumption in cluster formation and also CH election. The strong computation mechanisms are required to estimate the trust level of mobile node. Here, the trust value is estimated based on the public historical behaviors. Thus, it induces malicious node participation in data transmission and also introduces high packet loss. Message may be modified or false data packets can be injected by the malicious nodes in intermediate hops.

The problem statements of these researches insist the need of a secure data transmission protocol which routes data in the optimal way through the trustworthy nodes whose trustworthiness is evaluated with strong parameters. The problems stated are illustrated in Table I. In this way, our proposed system is carried out towards the solutions of these problems by improving the security and scalability of data transmission in MANET.

TABLE I. EXISTING PROBLEMS

Method/ Technique	**Concept**	**Drawback**
B4SDC [29]	Detects collusion and spoofing attacks	The existing blockchain structure is not scalable furthermore; creating blocks for dense MANET consumes high energy
BP-AODV [30]	Blackhole attackers are detected through nodes past behaviors	The routing is not efficient since trustworthiness of the nodes is computed by considering only the historical behavior
Tanimoto SVM based linear program [31]	Classification of nodes based on node history and current energy status	Lack of mobility information leads to high data loss
Fuzzy logic based Clustering [32]	The trust nodes are determined by the cluster head	The number of fuzzy rules generated for CH election will make the process time consuming

IV. PROPOSED METHODOLOGY

The proposed system addresses challenging issues present in current MANET security works. The mobile ad-hoc network has become more popular in wide variety of applications that eventually increases intruders. This section is categorized into sub-sections depending on hierarchy of process involved to provide highly confidential authentication and data security in MANET that avoids severe attacks in network. In the present study, we have employed BDAG method to detect the malicious attacks mainly because of its relatively minimum resource utilization, fast detection of attacks and high delivery ratio.

A. B-DAG CHAIN Architecture

The proposed system comprises of four processes. The processing handled in each process is user validation, clustering, optimal route selection and data packet verification. The entities present in the proposed MANET environment are Security Node, Bayesian Network Directed Acyclic Graph aided Blockchain Nodes, and Mobile Nodes. The malicious traffic is provoked with the objective of demolishing the performance of the network. Initially the network consists of both the legitimate users and malicious users. Let the users be {U_1, U_2, U_3… U_n} in which the data transmission is to be done between the legitimate users so the authentication of the legitimate users is important in secure data transmission. The users who possess original security credentials are termed to be legitimate users. The security nodes present in the environment is denoted as {S_1, S_2… S_n}. The security credentials of the legitimate users are managed by the security nodes. Once the security node receives the credentials of the users it starts to compute the key for message signing process. The number of users in the MANET environment is huge and it is not possible to manage the users individually hence clustering of mobile nodes is introduced, this process significantly reduces the complexity of managing the mobile nodes. Fig. 1 depicts the system architecture of the proposed work. The cluster head is elected and it is managed by security node. In order to reduce the packet drops and retransmission of data packet the data packet transmission is to be done through trusted nodes. The reputation value of each node is estimated and the source node selects the forwarder based on the reputation. In the destination side, both the sender's authentication and integrity of data packets are verified and the timestamp is also checked for secure transmission of data. On designing the BDAG chain architecture, the malicious nodes are detected and several attacks caused by these nodes are defended. The user authentication is carried out by using CubeHash algorithm and bliss algorithm. Then clustering is done using weighted sum computing for clustering algorithm and finally the secure routing is carried out by using Dolphin Swarm Optimization. Fig. 1 shows the proposed BDAG chain architecture and the processing carried out in each process. All these processes are completely focused on mitigation of the attacks caused by the malicious nodes.

B. Multi-Factor Authentication

The U_n users of MANET environment are validated when the user requests with a service. User validation includes processing of two phases as (I) Registration phase and (II) Authentication phase. The steps in registration phase are given as follows.

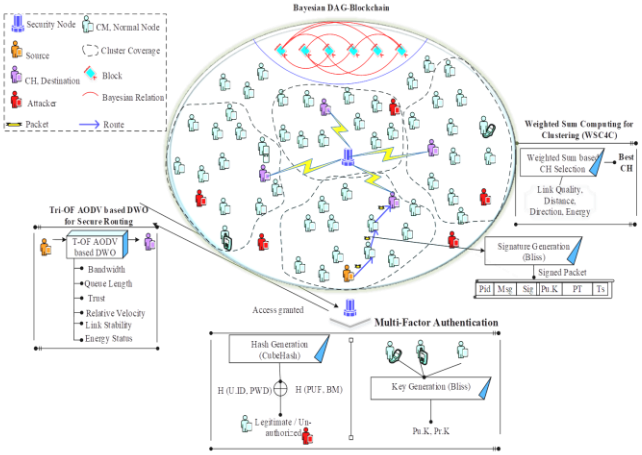


Fig. 1. System Architecture.

STEP 1: First assume U_1 be the user who requests the security node (SN) for registration with his / her unique Binary format of user finger vein, Physically Unclonable Function (PUF), Password and User ID. These credentials are submitted to SN for registration.

$$U_1\,(BM\|PUF\|PWD\|ID) \longrightarrow SN \quad (1)$$

STEP 2: Then, receiving user credentials from U_1, the SN generates hash value for all user credentials by using CubeHash algorithm. The parameters involved in CubeHash algorithm are listed below:

- RD - The number of iterations in {1to 16}.
- Bpb – It is represented in bits per packet block {1 to 128}.
- O – The output bits range from {2 to 512}.
- Pkt - the actual message as a string of bits in size {0 to 2^{128-1}}.

The algorithm involves the stages listed below:

- The state S is initialized based on (O, Bpb, RD)
- The Pkt should be divisible by Bpb for that padding may be performed.
- The RD rounds of the ordering on state S is performed for every Bpb-byte block in the padded O xored with first Bpb- bytes of state.
- The state S is then finalized.
- The final result is delivered as the first O bits of state S.
- Each state is built of 32 bits. The first three values are set to O/8, Bpb, RD in the initialization stage. Further the state is ordered to 10RD rounds. Until the value of Pkt is divisible by Bpb the padding is carried out by appending the pkt by 1. The preserved symmetry is broken by performing the XOR operation to the last bit with the integer value1. Finally, the state is reordered through 10RD rounds once again. CubeHash seems to easily configure the input parameters such as BM, PUF, PWD and ID. The maximum security is obtained by deploying CubeHash 8/1-512 and the energy efficiency is obtained by deploying CubeHash 16/32. The hash values H is determined which is used to generate the unique signature.

Procedure for Key Pair Generation

```
1: Begin
2: Initialize nodes
3: $\boldsymbol{U_1}$→ request key pairs to the $\boldsymbol{SN}$
4: SN (For $U_1$ generate key pairs)
    $\boldsymbol{hash\ value\ acquisition}$
    $\boldsymbol{Key\ pair\ generation}$(Pr.k, Pu.k)
5: End for
6: $\boldsymbol{SN}$→ reply key pairs to $U_1$
```

Procedure Description: The U_1 requests the key pairs to the security node which will be generated from the hash values determined for the user credentials. Once hash values are obtained the two different keys Pr.k and Pu.k are generated. The security node assigns the Pr.k and Pu.k to the user here it is U_1. Further the keys from SN are stored in user's device.

The BLISS algorithm is used to generate the digital signature. First, the two different keys Pr.k and Pu.k are generated. The Pr.k is a (short) matrix $S \in Z_{2q}^{mxn}$ and Pu.k is given by the matrix $A \in Z_{2q}^{n\times m}$ such that AS = q**I**n (mod 2q). The security node assigns the Pr.k and Pu.k to the user here it is U_1.

$$SN \longrightarrow U_1\,(Pr.k,\ Pu.k) \quad (2)$$

STEP 3: Further the keys from SN is stored in user's device which is required during the authentication process. The registration phase for the device is completed.

Procedure for Message packet transmission

```
1: Initialization
2: $U_1$ → requests for connection with $G_1$
3: Timestamp verification by $G_1$
4: $G_1$→ reply ack to $U_1$
5: $U_1$ (for message transmission)
    Message $\boldsymbol{\mu}$ is generated
    Signing of message with generated keys (Pr.k, Pu.k)
6: End for
7: $U_1$→ Message transmission to $G_1$
```

Procedure description: U_1 requests for the connection establishment with G_1. The timestamp for the request message is verifies by G1 and the ack for connection is sent to U_1. For message transmission the message μ is generated and the digital signature is signed with the key. The signed message is then transmitted to G_1 in several hops. The steps followed in authentication phase are described below:

STEP 1: During authentication the request from U_1 is submitted to G_1 for data transmission. On receiving request, the timestamp T_1 freshness is verified. Then the G_1 replies the U_1 with the acknowledgment (ack). Once the ack is received by the U_1, the message μ is generated and the private key is used to sign the message. The signed message is denoted as δ which is sent to the destination G_1

$$U_1(\mu \oplus Pr.k) \longrightarrow U_1\ (\delta\ ) \quad (3)$$

Procedure for Message packet reception

```
1: Reception
2: $G_1$ (For key generation)
    verification of sender identity ($U_1$)
    verification of data integrity (δ)
    Pr.k is generated for the destination node
3: End for
4: The message packet is decrypted
```

Procedure Description: After the reception of encrypted message packet the G_1 verifies the sender identity of the message and the data integrity of the packet. After the verification process, the private key is generated to decrypt the received message.

- STEP 2: The signed message packet is transmitted to the next reputed node and thus the message packet reaches the destination in several hops.

U_1 (δ) ⟶ G_1 (4)

STEP 3: Once the destination node receives the packet, the private key for the respective message packet is generated to the destination. This way of data transmission provides security to the transmitted data effectively.

$$G_1(\delta) \longrightarrow G_1(\mu \oplus Pr.k) \quad (5)$$

The authentication of users enables to withhold illegitimate user's access into the network. A system model without authentication process is much easier for attackers to initiate attack which degrades network performance. The authentication of user by private and public key ensures to allow access only for the legitimate users. The goal of our work is to defend the attacks and to perform the data transmission securely.

C. Weighted Sum Computation for Clustering

The mobile nodes in the MANET environment are clustered to minimize the computation complexity. The clustering of nodes undergoes two phases they are (I) cluster head election and (II) cluster formation. The nodes are grouped based on the factors such as Energy status, distance, link quality and direction. The resulting cluster will contain single cluster head (CH) and number of cluster members. The cluster head has complete information about the cluster members and link state details. Each and every node in the cluster is connected to the cluster head with a bi-directional link, through this each node in the cluster knows which cluster it belongs to. The proposed Weighted Sum Computation. For Clustering (WSC4C) performs well in optimal cluster formation in highly moving MANET environment. The proposed algorithm computes the weight score for each factor and then elects the optimal node as cluster head.

1) Energy status calculation: The energy status for each node in the MANET environment is obtained by finding the difference of the energy availability in two sub-phases. The energy spent on forming the topology is considered to obtain the correct energy status of the mobile node. For that the energy status before topology formation and the energy spent on topology formation. The energy status can be found by the equation as follows:

$$E_{status} = E_{Bt} - E_{St} \quad (6)$$

2) Geometrical distance calculation: The distance between each node is to be found to decide the cluster size and the optimal cluster head for the respective cluster. The distance calculation is carried out in meters (m). The optimal distance between the node and the security node is calculated. The reason to calculate distance is that when the distance between two nodes is small the energy required in transmitting the packet between the nodes reduces. The geometrical distance between two nodes is calculated as follows:

$$D(t) = \sqrt{A1 + A2 + \theta} \quad (7)$$

3) Link quality estimation: The link quality is one of the significant parameters to be considered in highly moving MANET environment. The estimation of link quality is carried out through number of transmissions expected (NET) and the path count expected (PCE). The number of transmissions expected (NET) between the transmission of packets between sender and receiver is used to calculate the link quality. Let node U(i) be the intermediate node which has the probability of receiving and transmitting the message packets of $\alpha(i) and\ \beta(i)$ respectively. The probability of packet delivery ratio between the nodes is calculated as follows:

$$\alpha(i) = \frac{n_w}{w/_{\tau}} \quad (8)$$

The probability that a previous node sends packet to the node U(i) is stated as $P_{pre} = 1 - \Pi_{i>s}(1 - \alpha_s \beta_i)$ and the probability that the next node receives a packet from U(i) is stated as $P_{next} = 1 - \Pi_{d>i}(1 - \alpha_i \beta_d)$. Then the number of transmissions expected is determined by

$$\text{NET} = \frac{1}{Ppre \times Pnext} = \frac{1}{(1-\Pi_{i>s}(1-\alpha_s\beta_i))(1-\Pi_{d>i}(1-\alpha_i\beta_d))} \quad (9)$$

The PCE value is calculated based on the probability of packet delivery ratio. This metric is calculated to find the optimal pair of the node U(i). The PCE value from sender to receiver is can be calculated as

$$\text{PCE(s,d)} = \frac{1+\sum_i PCE\left(c_i^{s,d},d\right)(1-\Pi_{i>s}(1-\alpha_s\beta_i))\Pi_{j-1}^{i-1}(1-\Pi_{d>i}((1-\alpha_s\beta_j))}{1-\Pi_{s>i}(1-\alpha_s\beta_i)} \quad (10)$$

The above determined NET and PCE metrics are used to estimate the link quality between the nodes in the MANET environment.

4) Direction estimation: The direction of nodes in a MANET environment can be estimated from the change in link quality between the nodes. If the link quality increases between the nodes, then they are moving towards one another and if the link quality degrades between the nodes, then they are moving away from one another. Thus, the direction of the nodes can be classified into two classes they are (i) moving toward (TW) and (ii) moving away (AW). The weighted sum computation for clustering is carried out with the above calculated factors and the clustering is performed in an optimal manner. From the nodes present in the cluster, the cluster head (CH) is elected based on the calculated weighted sum. Table II illustrates the formation of cluster and election of cluster head based on WSM score. The node $U3$ is elected as the Cluster Head (CH), as the Weighted Sum Computation (WSC) score for the respective node is greater when compared to other nodes.

TABLE II. CLUSTER FORMATION AND CLUSTER HEAD SELECTION

Nodes	**Input parameters for clustering**				**WSC score**	**Role**
	C_1	C_2	C_3	C_4		
$U1$	5	12	75%	AW	0.75	CM
$U2$	8	10	78%	TW	0.82	CM
$\boldsymbol{U3}$	**11**	**3**	**90%**	$\boldsymbol{TW}$	**0.91**	**CH**
$U4$	6	8	83%	AW	0.69	CM
$U5$	9	15	67%	AW	0.56	CM

Once the cluster is formed, each node in the cluster will broadcast its neighbor table for every periodic time period as a hello message. After receiving hello message from the neighbor node, the respective nodes ID and role (CH or CM) will be registered in the neighbor table. These clusters are managed by the security nodes. If any attack patterns found by the security node, it will immediately isolate the particular malicious node and inform this message throughout the network. This way of forming the cluster and electing the cluster head is efficient and this will greatly minimize the complexity and overhead in packets and control message forwarding.

D. TRI-OF AODV based DSO for Secure Routing

In the MANET environment, communication is done by sharing message packets from one node to another node. In this work, Ad hoc On-demand Distance Vector (AODV) protocol which is a significant routing protocol in MANET is used. The AODV protocol overcomes the issues of mobile network such as high mobility, packet loss, etc. The AODV routes the message packets to the next node based on the trust value of the respective node. The trust value is classified into two types they are (i) direct trust and (ii) indirect trust. The direct trust is estimated by using the past behavior and successful transaction of the node whereas the indirect trust is provided by the security node. In order to achieve more secure message packet routing, we use Dolphin Swarm Optimization (DSO) algorithm. The proposed algorithm computes the reputation value for each node and forwards the message packets to the most reputed node. The algorithm is classified into three stages which are as follows:

- Search stage.
- Call stage.
- Response stage.

Search stage: In the search stage, the mobile node searches its neighbor node from the neighbor table. The algorithm obtains two nodes one is, the node which is selected by the source node and the second is the node which is recommended by another neighboring node. For each node U(i) (i= 1, 2, 3…N), two corresponding possibilities X_i (i=1 to N) and Y_i (i= 1, 2, 3…N). Where, X_i is the node selected by the source node and Y_i is the node recommended by the neighbor nodes. First the node U(i) calculates the fitness for the node selected by itself and then for the node recommended by the neighbor nodes. The comparison of both the fitness value will help the source node to select the best node. The fitness value is calculated based on the factors such as link stability, relative velocity, available bandwidth, energy, queue length, and trust.

For the node X_i that node U(i) gets, its fitness F_{xit} is calculated as follows:

$$Fxit = Fitness\ (Xi) \tag{11}$$

Then the fitness value for node Y_i is calculated as F_{yit} is calculated as follows:

$$Fyit = Fitness\ (Yi) \tag{12}$$

$$\text{If } F_{yit} > F_{xit} \tag{13}$$

Then Yi is replaced by Xi. Otherwise, Xi which is selected by the source node itself does not change. After the updation of the reputed node, the DSO enters into next stage.

Call stage: In the call stage, the source node U(i) informs the neighbor node about the result obtained in the search stage and requests the connection from the selected reputed node for data transmission. The transmission time matrix (TM) gets updated as follows:

$$TM_{U(i)} = \left[\frac{Dist}{speed}\right] \tag{14}$$

After the updation of the transmission time matrix gets updated and the DSO enters the next stage.

Response stage: The reply for the request sent to the reputed node is received by the source node and the message packet is generated and sent to the respective node. The reputed node receives the message packet from the source node within the mentioned transmission time matrix. (TM). When the time becomes.

$$TMU(i) = 0 \tag{15}$$

The reputed node will no longer get the message packet, which means that the message packet will be transmitted to the reputed node within the time. This process gets looped until the destination node receives the packet. In this process the trust values provided by the malicious nodes gets eliminated and the message is transmitted through the reputed nodes and reaches the destination node in the optimal time. The objectives achieved by the Dolphin Swarm Optimization is listed below:

- Low Relative Velocity and High Link Stability.
- High Available Bandwidth and High Energy.
- High Trust and Low Queue Length.

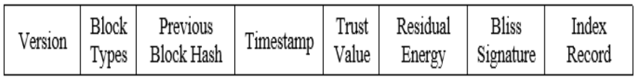
The Procedure 4 presents the overall working of DSO based AODV for multi-hop routing. The above explained three stages along with the start and end phase is involved for fitness computation of each relay node. In the start phase the mobile nodes are initialized with its input parameters. This process is significant for the initialization of parameters for fitness evaluation.

The best fitness function is chosen for packet transmission. The end condition is achieved when the packet reaches the destination. The matrix updation is done in both call stage and response stage which is done to make the routing process within the labeled time period.

```
Procedure: Route selection by DSO algorithm.
1: initialization
     Collects information about neighboring nodes from neighbor table
     Nodes= {U1, U2, U3...} in the neighbor table.
2: begin loop
     While the end condition is not satisfied do
2.1: search stage
     Two nodes Xi and Yi are obtained.
     Calculate fitness $F_{xit}$ and $F_{yit}$.
     Highest fitness node is selected.
2.2 Call stage
     Request for connection
     Update time matrix.
2.3 Response stage
     Reply received
     Packet generation
     Update time matrix.
3 If packet reached destination then
     End loop
Else
     Increment loop
End if
End while
End
```

E. Attacks Mitigation by Bayesian DAG-Blockchain

In this section, the attacks associated with the routing in MANET environment is explained briefly and a model is proposed to defend against these routing attacks. Generally, routing in mobile ad-hoc network is to be performed in an optimal way to reduce the latency and increase the privacy of the mobile nodes. Some of the nodes try to bypass the message packet to steal the sensitive information embedded in it; these nodes are collectively called as malicious nodes. To mitigate the attacks occurring in routing process, the Bayesian Direct Acyclic Graph (B DAG) aided Blockchain model is proposed. The security of the routing protocol is increased by using blockchain technology. The blockchain makes use of asymmetric encryption and authorization processing. Fig. 2(a) illustrates the format of the data block; (b) describes the individual specification of the data blocks.



Version	Block Types	Previous Block Hash	Timestamp	Trust Value	Residual Energy	Bliss Signature	Index Record

(a)

version	Block version number
Block types	Node details
Previous Block Hash	Link for connecting block
Timestamp	Block creation time
Trust value	Node trust
Residual energy	Energy availability
Bliss signature	Public and private key
Index record	Holds index information

(b)

Fig. 2. (a) Format of Data Block, (b) Data Block Description.

The transaction of packets stored on the blockchain is public, but the identity of the nodes is encrypted and the key for encryption is provided to the data owner only thereby ensuring the privacy. Each and every action in blockchain is transparent and is available to every node of the block however the data cannot be deleted or changed. The decentralized management of network reduces a number of risks that emerge with data being managed centrally. This type of management has no central point of failure. The priority of trust is given equally to all the nodes. The verification of message packet is performed to find whether the source of the packet is a legitimate user and the data integrity of the packet. To do so each and every event of all the nodes are stored in a chain of blocks. To eliminate the problem of storage requirement, these events are converted into hash values and these hash values are table verification process. The previous hash of the block is stored in the current block therefore the security of the blockchain increases with the number of blocks. Traditional blockchain technologies arrange the blocks in a single chain. So, in order to verify the packet integrity, the hash values of source to destination are to be verified and this will lead to delay in the verification process. To overcome this delay the blocks are presented in Direct Acyclic Graph (DAG). This enables the verification process to check the needed blocks only. But in order to select the required block, all the blocks associated with the process is to be checked. Therefore, a Bayesian Network is used to estimate the probability of the hash value in the respective block. This significantly reduces the delay associated with the process. The Block Independence value (BI) is presented as a triplet of $J\ (x, y, z)$. Here the value x denotes the key of $J(x, y, z)$. The factors determining the Block independency is listed as follows:

- Symmetry
- Decomposition
- Weak union
- Contraction

The graph is plotted for the number of blocks in a hyper tree construction ordering. The hyper graph is denoted as.

$$\langle B, P\rangle = \{b_1, b_2 \ldots b_n\} \tag{16}$$

Where, bi $\subseteq P$ is called a $hyper\ edge$ of ⟨B, P⟩, and P = $b_1 \cup b_2 \cup \ldots \cup b_n$. the hyper graph B is determined as acyclic if $, si = bi \cap\ (b_1 b_2 \ldots b_{i-1}) \subseteq b_j, 1 \leq j \leq i-1,$ where s is referred to as segregator. Thus, an acyclic hypergraph is constructed and thereby removing the dependency between each block in the blockchain.

V. Results and Discussion

This section presents the simulation results with the detailed description of three sub-sections include simulation setup, comparison analysis, security & efficiency analysis for the proposed model in comparison with the existing approaches.

A. Simulation Setup

The Network Simulator version 3 (NS3) is used to evaluate our proposed model. The hardware and software requirements for the proposed model are illustrated in Table III.

The mobile node configuration is deployed to transmit the data by sensing the varied circumstances. The network simulator 3 tool has better features of network and provides all specifications of MANET. The proposed B DAG aided blockchain based secure routing model is experimented in 1000m × 800m simulation environment for evaluation of packet transmission by defending various attacks. The codes implemented for the construction of clusters, route establishment for transmission of data. Secure routing is a significant factor which is considered in many research works and our work also focuses on secure routing in MANET environment. Table IV describes the parameters associated in the experiment of proposed work in simulation tool. Fig.3 illustrates the flow of the proposed work in the NS3 tool.

B. Comparison Analysis

This sub-section presents the formulation of the proposed B-DAG aided blockchain secure routing model with respect to several QoS metrics. The proposed research work is compared with several existing works. Particularly, the following metrics are considered for performance analysis: attack prediction rate, end to end delay, packet delivery ratio, route acquisition delay, routing overhead, security strength and throughput. These metrics are described in the following in detail.

TABLE III. SYSTEM CONFIGURATION

Hardware specifications	Processor	NS3.26
	RAM	2GB
	Hard Disk	60GB
Software Specifications	Network Simulator	Pentium Dual Core and Above
	OS	Ubuntu 14.04 LTS

TABLE IV. SIMULATION PARAMETERS

Parameters	**Description**
Simulation area	1000 m*800 m
Number of nodes	100 with 10% of attackers
Node mobility model	Random waypoint model
Node speed (Max)	5 m/s
Forwarding capacity	2 Mbps
Number of flows	50
Transmission range	250 m
Packet transmission average rate (per flow)	1024 bytes/packet
Node buffer size	64 packets (fixed)
Queue type	Priority queue
Traffic type	TCP, UDP, and ICMP
Nodes distribution	Random
Interface type	Physical wireless
Neighbor nodes waiting time	0.3 s
Duration for packets carrying	1 s
Propagation delay mode	Constant speed
MAC type	Ad Hoc Wi-fi MAC

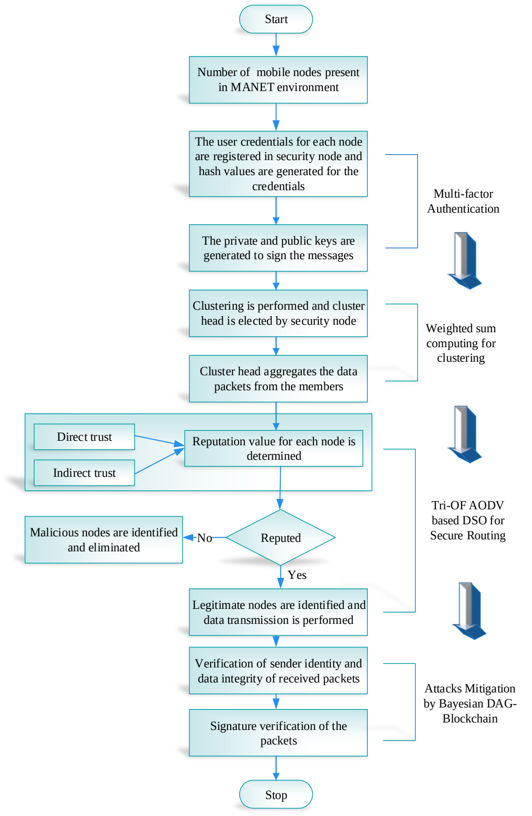

Start
Number of mobile nodes present in MANET environment
The user credentials for each node are registered in security node and hash values are generated for the credentials
The private and public keys are generated to sign the messages
Multi-factor Authentication
Clustering is performed and cluster head is elected by security node
Cluster head aggregates the data packets from the members
Weighted sum computing for clustering
Direct trust
Indirect trust
Reputation value for each node is determined
Malicious nodes are identified and eliminated
No
Reputed
Yes
Tri-OF AODV based DSO for Secure Routing
Legitimate nodes are identified and data transmission is performed
Verification of sender identity and data integrity of received packets
Signature verification of the packets
Attacks Mitigation by Bayesian DAG-Blockchain
Stop

Fig. 3. Flow of B-DAGChain Simulation.

1) Impact of attack prediction rate: Attack prediction rate is defined as the number of attacks predicted for the given unit time. The true positive value is used to compute the attacks. It is defined as the number of packets which are determined correctly as normal for the total number of packets forwarded. It is calculated as.

$$APR = \frac{no.of.detected\ attacks}{no.of.attacks} \times 100\% \tag{17}$$

$$APR = TPV = \frac{TP}{TP+FN} \tag{18}$$

Fig. 4 depicts the attack prediction rate of three works including the proposed work with respect to number of malicious nodes. With the implementation of B DAG aided Blockchain model, attack prediction rate gets improved for the proposed research work which is evaluated for different number of malicious nodes. This work primly focuses on prediction attacks caused by the malicious node and mitigation of those attacks Table V. Firstly, the packets are signed with the digital signature and then packets are forwarded through reputed nodes and reach the destination. Existing works such as B4SDC and BP-AODV considers the trust values of the malicious nodes.

2) Impact of end-to-end delay: The End-to-End delay is defined as the delay of packets between two nodes. The end-to-end delay is calculated with respect to number of nodes.

Fig. 5 depicts the end-to-end delay the proposed method in comparison to the existing works for increasing number of nodes. The proposed work implements clustering of nodes using Weighted Sum Computing for Clustering (WSC4C) algorithm which will reduce the complexity and delay associated with quantity of nodes Table VI. In the existing works [29], [30] the delay increases exponentially with increase in the number of nodes.

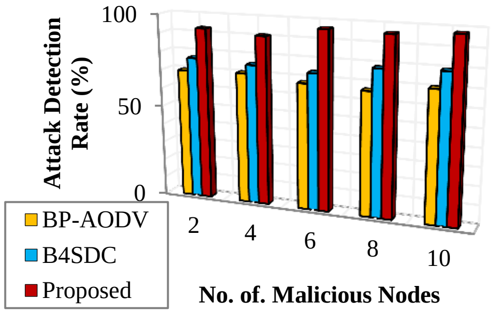


Fig. 4. Attack Prediction Rate vs. no. of. Malicious Nodes.

TABLE V. COMPARISON OF ATTACK DETECTION RATE OF PROPOSED METHOD WITH EXISTING METHODS FOR DIFFERENT NUMBER OF MALICIOUS NODES

No of Malicious Node	**Attack Detection Rate (%)**		
	BP-AODV	**B4SDC**	**Proposed**
2	69.7	76.7	92.9
4	70.5	75.3	90.8
6	67.8	73.5	96.3
8	66.5	78.3	95.7
10	70.3	79.4	97.7

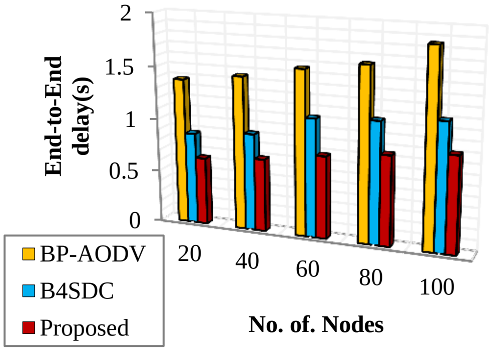


Fig. 5. End-to-End Delay vs. no. of. Nodes.

TABLE VI. COMPARISON OF END-TO-END DELAY OF PROPOSED METHOD WITH EXISTING METHODS FOR DIFFERENT NUMBER OF NODES

No. of Nodes	**End-to-End Delay(s)**		
	BP-AODV	**B4SDC**	**Proposed**
20	1.38	0.87	0.64
40	1.45	0.92	0.69
60	1.56	1.12	0.78
80	1.64	1.15	0.85
100	1.85	1.2	0.91

3) Impact of packet delivery ratio: Packet Delivery Ratio (PDR) is termed as the ratio between the numbers of packets delivered with respect to the number of malicious nodes present in the MANET environment. Fig 6 depicts the performance of proposed method in terms of packet delivery. With the increased number of malicious nodes, the existing systems [29], [30] fails to achieve better packet delivery ratio. The proposed work uses Dolphin Swarm Optimization (DSO) for reputed node selection and AODV protocol for secure route selection and this eliminates the trust provided by the malicious nodes thereby not affecting the packet delivery ratio Table VII.

4) Impact of security strength ratio: Security Strength is described as the level of security provided to the sensitive information embedded into the message packet. The security strength is improved by authentication of legitimate users and encryption of message packets during transmission of packets. Fig. 7 depicts the comparison of security strength provided by the proposed methods and other existing methods with respect to the packet size. The proposed method proves to be more secure even when the size of the packets is increased. The Bayesian Direct acyclic graph aided blockchain technology implemented in the proposed work improves the security of routing Table VIII. The existing works fails to focus on security when the packets and number of nodes increase which is a significant drawback.

5) Impact of throughput: Throughput is defined as the rate of successful reception of message packets by the destination node. It is one of the important factors in determining the accuracy and safety of the research work. Fig. 8 depicts the throughput achieved by the packets with respect to the increasing number of malicious nodes in three research works. This shows that the proposed work has higher throughput rate when compared with other research works. The proposed work uses DSO in selecting the reputed nodes thereby eliminating the malicious nodes which will reduce the number of packets drop and other adversary activities. The existing works are attracted by the smaller number of hop counts presented by the attackers and considers the trust value provided by them but the proposed work calculates the reputation value based on several features including the indirect trust provided by the security node Table IX. Therefore, it is able to differentiate the malicious nodes from the legitimate nodes. Thus, the proposed work has better throughput.

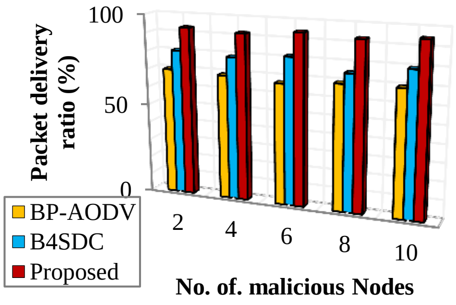


Fig. 6. Packet Delivery Ratio vs. no. of. Malicious Nodes.

TABLE VII. COMPARISON OF PACKET DELIVERY RATIO OF PROPOSED METHOD WITH EXISTING METHODS FOR DIFFERENT NUMBER OF MALICIOUS NODES

No. of Malicious Nodes	Packet Delivery Ratio(%)		
	BP-AODV	B4SDC	Proposed
2	69.8	80.5	93.2
4	68.7	78.9	91.9
6	66.8	81.3	94.3
8	69.2	74.9	92.8
10	69.5	79.4	94.7

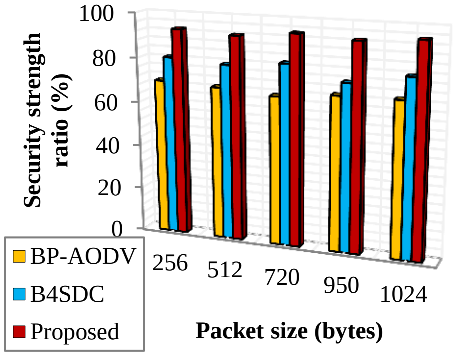


Fig. 7. Security Strength Ratio vs. Packet Size.

TABLE VIII. COMPARISON OF SECURITY STRENGTH RATIO OF PROPOSED METHOD WITH EXISTING METHODS FOR DIFFERENT NUMBER OF PACKET SIZE IN BYTES

Packet Size (Bytes)	Security Strength ratio (%)		
	BP-AODV	B4SDC	Proposed
256	69.8	80.5	93.2
512	68.7	78.9	91.9
720	66.8	81.3	94.3
950	69.2	74.9	92.8
1024	69.5	79.4	94.7

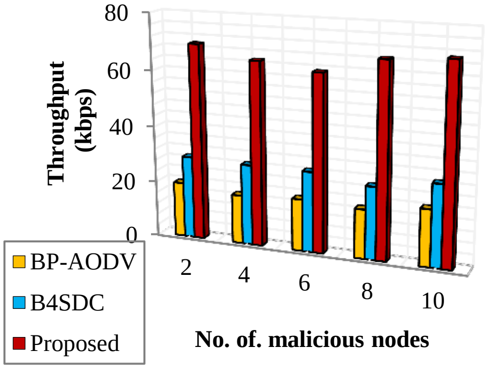


Fig. 8. Throughput vs. no. of. Malicious Nodes.

TABLE IX. COMPARISON OF THROUGHPUT OF PROPOSED METHOD WITH EXISTING METHODS FOR DIFFERENT NUMBER OF MALICIOUS NODES

No. of Malicious Nodes	Throughput(kbps)		
	BP-AODV	B4SDC	Proposed
2	19.6	29.4	69.7
4	17.4	28.7	65.3
6	18.5	28.6	62.9
8	17.5	25.8	68.7
10	20.2	29.2	70.2

6) Impact of routing overhead: Routing Overhead is defined as the ratio of number of packets generated to the number of packets transmitted in the established route. The routing overhead depends on the link stability and quality. The number of nodes and mobility of nodes also influences the routing overhead. Fig. 9 depicts the performance of proposed work in terms of routing overhead with respect to number of nodes. This shows that the proposed work has less routing overhead when compared to the other existing works, this is because the proposed work implements the clustering process by using Weighted Sum Computation for Clustering (WSC4C) to cluster the nodes in the MANET network thereby increasing the link quality between the nodes which will reduces the routing overhead Table X.

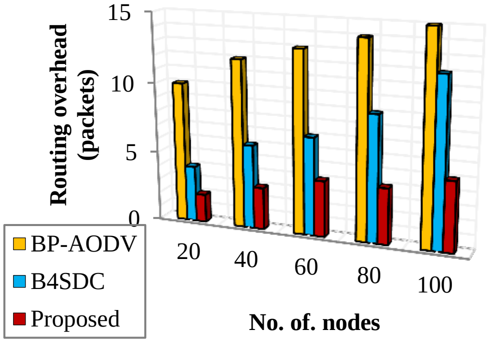


Fig. 9. Routing Overhead vs. no. of. Nodes.

TABLE X. COMPARISON OF ROUTING OVERHEAD OF PROPOSED METHOD WITH EXISTING METHODS FOR DIFFERENT NUMBER OF NODES

No. of Nodes	Routing Overhead (Packets)		
	BP-AODV	B4SDC	Proposed
20	10	4	2
40	12	6	3
60	13	7	4
80	14	9	4
100	15	12	5

7) Impact of routing acquisition delay: Route Acquisition is described as the establishment of route between two nodes for forwarding the data packets from source to destination. The delay associated with the route establishment is termed as route acquisition delay. This delay is occurred mainly due to lack of selection of neighboring nodes. Fig. 10 depicts the comparison of route acquisition delay in three research works including the proposed work with respect to the routing hops. Existing works focuses on only the selection of neighbor nodes based on the trust value but the selected node may not have sufficient energy level to forward the packet and this will lead to route acquisition delay Table XI. The proposed work selects the reputed neighbor node based on link stability, relative velocity, available bandwidth, energy, queue length, and trust. Hence the delay associated with route acquisition is decreased significantly.

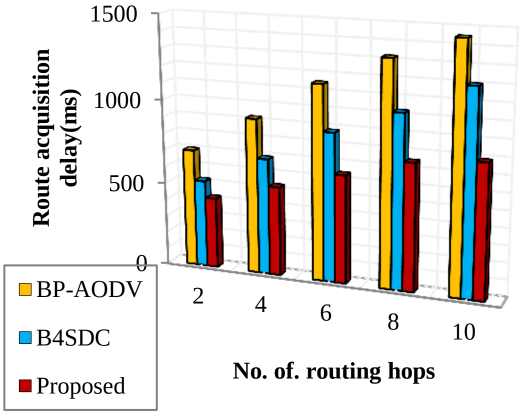


Fig. 10. Routing Acquisition Delay vs. no. of. Routing Hops.

TABLE XI. COMPARISON OF ROUTING ACQUISITION DELAY OF PROPOSED METHOD WITH EXISTING METHODS FOR NUMBER OF ROUTING HOPS

No. of Routing Hops	**Routing Acquisition Delay(ms)**		
	BP-AODV	**B4SDC**	**Proposed**
2	700	520	420
4	920	690	530
6	1150	880	640
8	1320	1024	750
10	1450	1200	790

C. Security and Efficiency Analysis

The packet transmission in the MANET environment carries sensitive data and the security of these message packets should be ensured. The malicious nodes in the network lead to routing issues. The attacks caused by these nodes will affect the performance of routing between the nodes and greatly affects the privacy of the nodes. Some of the important routing attacks and the process followed by the proposed work to overcome these attacks are explained below:

Black Hole attack: In this type of attack, the attacker will attract the source node with low hop routes. Once the sender begins to transmit data packets, the attacker will drop the packets without transmitting it to the next node. This increases the latency among the nodes. The proposed system selects the reputed node for pack forwarding by considering both the direct and indirect trust of each node thereby identifying the false trust given by the malicious nodes.

Grey Hole attack: This is an advanced level of black hole attack in which the malicious node will behave like a legitimate node. Not all the packets send through this node will be dropped, the attacking node drops only the sensitive packets. These types of nodes are difficult to identify. However, the indirect trust provided by the security node will identify the symmetrical pattern of packet drop through which the grey hole attacks can be identified and the proposed method will eliminate these nodes during packet forwarding.

Worm Hole attack: A tunnel like structure is created by two or more nodes thereby decreasing the hop count of the route. Once the source node begins to transmit the packet through this tunnel, the source node gets attacked resulting in denial of service and replay attacks. The proposed work performs clustering of mobile nodes and the cluster head is elected for each cluster. The cluster head will have the link details of each node by doing so the nodes involved in these types of attacks can be identified and are eliminated during packet transmission.

Timing attack: in this type of attack, the attacker alters the time slot of the packet passing through it thereby causing a delay to the packet in reaching the destination. Due to this manipulation the receiver may not receive the packets on time. The proposed work identifies the malicious node even before the attack takes place, hence these types of attacks can be avoided.

Intruder attack: In this type of attack, the attacker is from outside the network. These attackers enter the network by manipulating the user present in the network. Once the malicious nodes enter the network they start to attract the source nodes which will leads to packet drop and security threat to the sensitive information. The proposed method secures the authenticity of the user through multi factor registration and authentication. The credentials such as Binary format of user finger vein, Physically Unclonable Function (PUF), Password and User ID are registered hence the manipulation of malicious nodes is prevented.

The efficiency of the proposed work is expressed in terms of QoS, energy consumption and security which is depicted in Fig. 4 to 10. The proposed work has better performance when compare to existing works which is explained in terms of security strength ratio, routing overhead ratio, packet delivery ratio, attack prevention rate, end-to-end delay, throughput, route acquisition time. The summary of the proposed research work is briefed as follows:

- The user identity ID registered and the hash values for these credentials are generated by using CubeHash algorithm. These hash values are used to create the private and public keys for the encryption of the message packets during transmission.

- The network complexity and the transmission overhead are minimized by forming the cluster of nodes by using Weighted Sum computation for Clustering (WSC4C). Factors such as energy status, geometrical distance, link quality and moving direction are computed and the weighted sum of these factors is used for cluster formation and cluster head election.

- The routing of message packets is done through the reputed nodes which are selected using Dolphin Swarm Optimization (DSO) algorithm. The reputed nodes are estimated based on link stability, relative velocity, available bandwidth, energy, queue length, and trust. Through this algorithm the high link stability, low queue length and high bandwidth is achieved.

- The attack mitigation is carried out by Bayesian Direct Acyclic Graph aided Blockchain. The verification of the received packet is taken place by examining the user authentication and integrity of the data. Once the verification process is over the key to decrypt the received message packet is generated. The blocks in the blockchain technology are distributed in the hyper graph and the block independency of each block is determined thereby the proposed work improves the performance of the process.

VI. Conclusion

In this work, Dolphin swarm optimization is proposed to improve the secure routing in MANET environment. To achieve the highly secure routing of data packets the Blockchain technology is used. Each and every transaction of the nodes in the network gets stored in the blocks and the hash values for these events are generated in the blocks. The user legitimacy is verified by multi-factor authentication of user. The credentials such as Binary format of user finger vein, Physically Unclonable Function (PUF), Password and User ID are collected and hash values are created by using CubeHash algorithm. These hash values are used to generate the keys to encrypt the message packet. Then the mobile nodes are clustered by using Weighted Sum Computation for Clustering to minimize the complexity encountered in routing data packets. The node with the high WSM score is elected as the cluster head. The routing is taken placed through reputed nodes which are selected by using Dolphin Swarm Optimization (DSO) algorithm. In the destination side the packets are verified for user authentication and integrity of data and the decryption of message packets is carried out by using Bayesian Acyclic Graph aided Blockchain technology. The block independence of the blockchain is computed which will improve the security of the routing in MANET environment. In future, the work can be extended by implementing the present method in MANET-IOT and also in view of improving its performance further by integrating diverse DLT algorithms.

References

[1] Narayana, V., & Midhunchakkaravarthy, D. (2020). A Time Interval based Blockchain Model for Detection of Malicious Nodes in MANET Using Network Block Monitoring Node. 2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA), 852-857.

[2] Careem, M.A., & Dutta, A. (2020). Reputation based Routing in MANET using Blockchain. 2020 International Conference on COMmunication Systems & NETworkS (COMSNETS), 1-6.

[3] Murugan, S., & Jeyakarthic, M. (2020). An Energy Efficient Security Aware Clustering approach using Fuzzy Logic for Mobile Adhoc Networks. 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC), 551-555.

[4] Sharma, V., Renu, & Shree, T. (2020). An adaptive approach for Detecting Blackhole using TCP Analysis in MANETs. 2nd International Conference on Data, Engineering and Applications (IDEA), 1-5.

[5] Pandey, S., & Singh, V. (2020). Blackhole Attack Detection Using Machine Learning Approach on MANET. 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC), 797-802.

[6] Shrestha, S., Baidya, R., Giri, B., & Thapa, A. (2020). Securing Blackhole Attacks in MANETs using Modified Sequence Number in AODV Routing Protocol. 2020 8th International Electrical Engineering Congress (iEECON), 1-4.

[7] Elhoseny, M., & Shankar, K. (2020). Reliable Data Transmission Model for Mobile Ad Hoc Network Using Signcryption Technique. IEEE Transactions on Reliability, 69, 1077-1086.

[8] Chetna, Ramkumar, K., & Jain, S. (2020). Performance Comparison of Spline Curves and Chebyshev Polynomials for Managing Keys in MANETs. 2020 7th International Conference on Computing for Sustainable Global Development (INDIACom), 64-67.

[9] Fasunlade, O., Zhou, S., & Sanders, D. (2020). Comprehensive Review of Collaborative Network Attacks in MANET. 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC), 1542-1545.

[10] Xia, H., Li, Z., Zheng, Y., Liu, A., Choi, Y., & Sekiya, H. (2020). A Novel Light-Weight Subjective Trust Inference Framework in MANETs. IEEE Transactions on Sustainable Computing, 5, 236-248.

[11] Biswas, A.K., & Dasgupta, M. (2020). A Secure Hybrid Routing Protocol for Mobile Ad-Hoc Networks (MANETs). 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), 1-7.

[12] Olanrewaju, R.F., Khan, B.U., Anwar, F., Mir, R.N., Yaacob, M., & Mehraj, T. (2019). Bayesian Signaling Game Based Efficient Security Model for MANETs.

[13] Veeraiah, N., & Krishna, B.T. (2020). An approach for optimal-secure multi-path routing and intrusion detection in MANET. Evolutionary Intelligence, 1-15.

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

[15] Alappatt, V., & Joe Prathap, P. M. (2020). Hybrid cryptographic algorithm based key management scheme in MANET. Materials Today: Proceedings. doi:10.1016/j.matpr.2020.09.788.

[16] Singh, N. C., & Sharma, A. (2020). Resilience of mobile ad hoc networks to security attacks and optimization of routing process. Materials Today: Proceedings. doi:10.1016/j.matpr.2020.09.622.

[17] Sharifi, S.A., & Babamir, S.M. (2020). The clustering algorithm for efficient energy management in mobile ad-hoc networks. Comput. Networks, 166.

[18] Chen, Z., Zhou, W., Wu, S., & Cheng, L. (2020). An adaptive on-demand multipath routing protocol with QoS support for high-speed MANET. IEEE Access, 1–1.

[19] Ali Zardari, Z., He, J., Zhu, N., Mohammadani, K., Pathan, M., Hussain, M., & Memon, M. (2019). A Dual Attack Detection Technique to Identify Black and Gray Hole Attacks Using an Intrusion Detection System and a Connected Dominating Set in MANETs. Future Internet, 11(3), 61.

[20] Devika, B., & Sudha, P. N. (2019). Power optimization in MANET using topology management. Engineering Science and Technology, an International Journal, 23(3), 565-575.

[21] Vinoba, R., & Vijayaraj, M. (2020). Novel control topology with obstacle detection using RDPSO - GBA in mobile AD-HOC network. Computer Communications.

[22] Jevtic, Nenad & Malnar, Marija. (2019). Novel ETX-based metrics for overhead reduction in dynamic ad hoc networks. IEEE Access. PP. 1-1.

[23] Alnumay, W., Ghosh, U., & Chatterjee, P. (2019). A Trust-Based Predictive Model for Mobile Ad Hoc Network in Internet of Things. Sensors, 19(6), 1467.

[24] Usman, M., Jan, M.A., He, X., & Nanda, P. (2020). QASEC: A secured data communication scheme for mobile Ad-hoc networks. Future Gener. Comput. Syst., 109, 604-610.

[25] Khan, B.U., Anwar, F., Olanrewaju, R., Pampori, B.R., & Mir, R.N. (2020). A Game Theory-Based Strategic Approach to Ensure Reliable Data Transmission With Optimized Network Operations in Futuristic Mobile Adhoc Networks. IEEE Access, 8, 124097-124109.

[26] Rani, P., Kavita, .., Verma, S., & Nguyen, G. (2020). Mitigation of Black Hole and Gray Hole Attack Using Swarm Inspired Algorithm With Artificial Neural Network. IEEE Access, 8, 121755-121764.

[27] Wang, X., Zhang, P., Du, Y., & Qi, M. (2020). Trust Routing Protocol Based on Cloud-Based Fuzzy Petri Net and Trust Entropy for Mobile Ad hoc Network. IEEE Access, 8, 47675-47693.

[28] Riasudheen, H., Selvamani, K., Mukherjee, S., & Divyasree, I.R. (2020). An efficient energy-aware routing scheme for cloud-assisted MANETs in 5G. Ad Hoc Networks, 97.

[29] Liu, G., Dong, H., Yan, Z., Zhou, X., & Shimizu, S. (2020). B4SDC: A Blockchain System for Security Data Collection in MANETs. IEEE Transactions on Big Data, 1-1.

[30] El-Semary, A.M., & Diab, H. (2019). BP-AODV: Blackhole Protected AODV Routing Protocol for MANETs Based on Chaotic Map. IEEE Access, 7, 95197-95211.

[31] Josephine, J., & SenthilKumar, S. (2020). Tanimoto Support Vector Regressive Linear Program Boost Based Node Trust Evaluation for Secure Communication in MANET. Wireless Personal Communications, 1-21.

[32] NagendranathMVS, S., & Babu, A.R. (2020). An efficient mobility aware stable and secure clustering protocol for mobile ADHOC networks. Peer-to-Peer Networking and Applications, 13, 1185-1192.