Computers, Materials & Continua
DOI: 10.32604/cmc.2023.032140
Article

Tech Science Press

EsECC_SDN: Attack Detection and Classification Model for MANET

Veera Ankalu Vuyyuru[1], Youseef Alotaibi[2], Neenavath Veeraiah[3,*], Saleh Alghamdi[4] and Korimilli Sirisha[5]

[1]Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram, 522502, A.P, India
[2]Department of Computer Science, College of Computers and Information Systems, Umm Al-Qura University, Makkah, 21955, Saudi Arabia
[3]Department of Electronics and Communications, DVR & DHS MIC Engineering College, Kanchikacharla, 521180, A.P, India
[4]Department of Information Technology, College of Computers and Information Technology, Taif University, Taif, 21944, Saudi Arabia
[5]Department of Electronics and Communications, BVC Institute of Technology & Science, Amalapuram, 533221, A.P, India
*Corresponding Author: Neenavath Veeraiah. Email: neenavathveeru@gmail.com

Received: 08 May 2022; Accepted: 16 June 2022

Abstract: Mobile Ad Hoc Networks (MANET) is the framework for social networking with a realistic framework. In the MANET environment, based on the query, information is transmitted between the sender and receiver. In the MANET network, the nodes within the communication range are involved in data transmission. Even the nodes that lie outside of the communication range are involved in the transmission of relay messages. However, due to the openness and frequent mobility of nodes, they are subjected to the vast range of security threats in MANET. Hence, it is necessary to develop an appropriate security mechanism for the data MANET environment for data transmission. This paper proposed a security framework for the MANET network signature escrow scheme. The proposed framework uses the centralised Software Defined Network (SDN) with an ECC cryptographic technique. The developed security framework is stated as Escrow Elliptical Curve Cryptography SDN (EsECC_SDN) for attack detection and classification. The developed EsECC-SDN was adopted in two stages for attack classification and detection: (1) to perform secure data transmission between nodes SDN performs encryption and decryption of the data; and (2) to detect and classifies the attack in the MANET hyper alert based Hidden Markov Model Transductive Deep Learning. Furthermore, the EsECC_SDN is involved in the assignment of labels in the transmitted data in the database (DB). The escrow handles these processes, and attacks are evaluated using the hyper alert. The labels are assigned based on the k-medoids attack clustering through label assignment through a transductive deep learning model. The proposed model uses the CICIDS dataset for attack detection and classification. The developed framework EsECC_SDN's performance is compared to that of other classifiers such as AdaBoost, Regression, and Decision Tree. The performance of the

This work is licensed under a Creative Commons Attribution 4.0 International License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

proposed EsECC_SDN exhibits ∼3% improved performance compared with conventional techniques.

Keywords: MANET; security; classifier; cryptography; attack; escrow; ECC

1 Introduction

Mobile Ad Hoc Network (MANET) comprises a vast range of mobile nodes to establish the network connection based on the demand in the network. Within the MANET environment, every packet in the network act as a router [1]. Furthermore, MANET has been widely utilized in a vast range of applications such as disaster management, military, personal area, networks, and so on. MANET environment comprises the dynamic or mobile environment with the estimation of failure point detection in the mobile ad-hoc environment [2]. However, the effective design of the protocol is involved in the transmission of packets in a dynamic environment between sender to receiver in topology. MANET environment comprises of the different categories such as the reactive, proactive, and hybrid environment. MANET environment provides connection-less, server, and permanent models in the centralized environment for dynamic access of data in a remote-control environment for improved security [3]. The functionality of MANET comprises the data blockage and time for the communication environment. MANET network offers a realistic framework with a broad range of social networking environments. The data transmission in the network is involved in information transmission based on reaction and query [4].

To improve the trusted user's privacy, needs to be maintained for effective maintenance of security. In a multi-hop MANET environment, explored packets need to be concerned about reaching the destination within the stipulated period. It is thought to be necessary for the construction of networks that connect nodes that are cooperative with one another [5]. In a MANET environment, data transmission routing is considered an effective parameter for the identification of optimal paths between nodes. The optimal performance of MANET is increased with spatial reusability of the nodes with increased throughput and end-to-end packet delivery [6]. Generally, the MANET is subjected to a vast range of security issues like the overflow of the routing table, wormhole, poisoning, snooping, packet replication, and denial of service (DoS).

The attacks affect the data transmission path between nodes to reach the destination without packet dropping [7–9]. Those attacks can be either single or collaborative in the case of single; in which packets are dropped independently, those are forwarded to the neighbors. In collaborative attacks, malicious nodes cooperate with packet dropping with the elimination of detection time [10]. To achieve the desired security in MANET, secure data transmission needs to be achieved using the cryptographic method. A similar key distribution within the network needs to be achieved. However, key distribution is a challenging task in the MANET environment. Usually, key management is involved in key setting, distribution of keys, and reversals of keys. In addition, this cryptographic scheme is subjected to the challenge of load balancing for handling public keys [11].

This research concentrated on improving security in the MANET environment due to the mobility and openness of the network. To achieve security in the MANET environment, this paper incorporates the following things.

- This paper incorporates SDN architecture to maintain the architecture of the MANET environment.

- In this paper escrow-based, Elliptical Curve Cryptography (ECC) is applied for data encryption. The generated keys are updated in the SDN for MANET security.
- To detect the attack transductive attacks integrated with Hidden Markov model (HMM) with hyper alerts.
- Within the transductive matrix, k-centroids are implemented for examination of attacks in the network.
- To classify the attack Intrusion Detection Evaluation Dataset (CIC-IDS2017) [12] is utilized for detection of attack in the MANET.
- The performance of the proposed EsECC_SDN is evaluated under two scenarios with attackers and without attackers. Finally, the proposed EsECC_SDN is a classifier based on a Support Vector Machines (SVM) classifier for attack classification.

This paper is organized as follows: In Section 2, related works are presented. The proposed EsECC_SDN for MANET with hidden Markov model (HMM) and transductive model for security is presented in Section 3. The simulation setting and classification of attacks are presented in Section 4 followed by the overall conclusion in Section 5.

2 Related Works

A MANET subjected to challenge of security to achieve desired communication performance of the network. This section provides the data transmission scheme between the nodes and the security scheme.

In [13], the authors developed a security scheme for MANET focused on DDoS attack prevention. The model involved in classification of DDoS attack with uses of dataset LIBSVM. The dataset for examination is generated through NS2 simulator for prediction accuracy. The testing and validation of the dataset s based on the consideration of bit rate, delay and packet delivery ratio PDR. The analysis expressed that the characteristics of the DDoS attack is minimal traffic network. However, the developed model involved in reduction of overall accuracy of the network.

In [14], the authors proposed a Diffie-Hellman method of key exchange and elliptic curve cryptography (HDHECC) for reliable data transmission with cryptography algorithm. Initially, the proposed HDHECC perform clustering with Low-energy adaptive clustering hierarchy (LEACH) protocol with selection of head with assigned weights in each node. Moreover, the proposed HDHECC incorporates trust mechanism for management of keys to retain public keys in the member node. With centralized key management public key are stored for estimation of packet loss, end-to-end delay and Packet delivery ratio. Similarly, in [15], the authors implemented multicast delay with cooperative multicast scheme for routing in MANET. The developed multicast algorithm with implementation of two-hop relay, where the packet transmitted between relay nodes to source node. The destination node involved in reception of packet from source node to the relay nodes. With implementation of multi-cast scheme cooperation and non-cooperation scheme is implemented for unicast algorithm with destination node those are equal to one. Furthermore, theoretical based Markov model cooperative multicast scheme for characterization of packet delivery.

To increase the overall security in the MANET network, in [16] the authors developed a modified ad-hoc on-demand multipath distance vector (AOMDV). The AOMDV model involved in detection of black hole attack in MANET for secure data transmission. In addition, AOMDV comprises of multi path message transmission for secure data with homomorphic encryption scheme. The examination of the results expressed that the PDR and throughput is higher. In [17], the authors examined the different

MANET attacks for the security improvement than the conventional technique. The performance of the network is computed based on the estimation of routing table with minimal delay. The MANET efficiency is based on consideration of the different factors such as flow rate, mobility, traffic, attackers, and position of nodes. Similarly, in [18], the authors presented a decentralized traffic monitoring system based on optimization model. The optimization-based approach uses bio-inspired algorithm stated as Artificial Immune System Based Algorithm (AISBA).

The proposed AISBA algorithm incorporates Artificial Immune System (AIS) for estimation of selfish and genuine nodes. With implemented protocol design, PDR is achieved as 93.47%. In [19], the authors focused on optimization and secure routing in MANET environment. The optimal routing in MANET is achieved through Ant Colony Optimization (ACO) for improved routing through estimation of difficulties in the network. To evaluate the network complexity, fuzzy logic model is implemented termed as Safety Aware Fuzzy Enhanced Ant Colony Optimization (SAFEACO) for effective routing in the network. The designed SAFEACO exhibits significant performance for the black hole, Sybil and inundation attacks in the network with computation of PDR and end-to-end delay.

In addition, in [20], the authors evaluated the MANET network performance based on Ad hoc On-Demand Distance Vector Routing (AODV), Dynamic Source Routing (DSR) reactive protocols. The evaluation is based on consideration of QoS matrices for guaranteed sensitivity level. The estimation is based on the consideration of node (PHY) layer. The estimation is based on the consideration of end-to-end delay, PDR and control overhead. In [21], computation is performed based on the peer-to-peer computing in the MANET. The performance is based on overlay participating peers (OPPs) for efficient processing in the MANET environment. With increase in node mobility overlay of protocol is minimized with increased maintenance, computation, control overhead, and lookup latency. In [22], the authors developed a AODV-BS protocol for prevention of black hole attack in MANET environment. The estimation is based on the consideration of different MANET model for normalization of the routing. The performance of the MANET is computed for the normalized routing, network delay and packet delivery ratio. Tab. 1 shows the summary of the literature.

Table 1: Summary of literature

Reference	Published year	Method	Outcome
[13]	2020	Prevention of DDoS attack in MANET	To prevent DDoS attack with improved performance
[14]	2020	To design effective cryptographic scheme for MANET	It offers desire key management scheme
[15]	2020	To perform multi-cast secure data transmission	Multi-cast scheme offers multi-cast communication
[16]	2020	To develop secure algorithm for Ad-hoc demand protocol	Developed a homomorphic scheme for security
[17]	2021	Reviewed the security threats and challenges in MANET	Reduced end-to-end delay and traffic load
[18]	2022	To implement optimization-based security model for MANET	Effectively identifies the selfish nodes

(Continued)

Table 1: Continued

Reference	Published year	Method	Outcome
[19]	2020	To develop secure optimization model	Effectively prevents black hole, sybil and inundation
[20]	2021	Self-configured secure routing scheme	Improved throughput and PDR
[21]	2021	Constructed routing model for MANET	Routing overhead is minimal
[22]	2020	Prevention of blackhole attack	Provides security

3 Security Scheme in MANET

The proposed escrow technique comprises the trustworthy SDN environment for security enhancement with the classification of attacks in the MANET [23–32]. The SDN acts as a centralized environment for data transmission and reception between nodes. With the SDN, the environment performs encryption and decryption. The environment of MANET is focused on improving authentication, confidentiality, integrity, and availability [33–42].

- Authentication–The legitimacy of the engaged data source that needs to be authenticated.
- Confidentiality–The system that involved in data processor execution in a devices.
- Integrity–The unauthorized user information is
- modified or corrupted.
- Availability–The capability of a network involved in the provision of appropriate services.

The proposed EsECC_SDN comprises five phases. The five steps involved in the model are Setup Phase, Key Generation, Encryption, decryption of node phase and decryption of the head phase. The proposed escrow scheme uses third party identification with the SDN controller. With SDN architecture MANET, network environment involved in the provision of global, versatility, optimization, and process. The proposed EsECC_SDN incorporates limited availability of resources and an appropriate strategy for connectivity for an unfeasible environment. The constructed escrow comprises the networking scenario with a structured, hierarchical, configuration of the separate data in the control plane.

3.1 ESECC_SDN Cryptographic Scheme for Security

The proposed EsECC_SDN comprises the 5 phases those need to be encrypted and decrypted through ECC [43–53]. The basic scenario in the encryption and decryption process is presented in Eq. (1)

$$I = \{setup,\ Encrypt,\ decrypt,\ SDN\ decrypt\} \tag{1}$$

Consider the two prime numbers p and q with the bit size of k (i.e., $2^{k-1} < p, q < 2^k$). The generated random numbers are stated as $N = \ p^2 q$ with the random component value of $g \in Z_n$ and the order is stated as $g_p \ := \ \ g^{p-1} mod\ p^2$. Based on the computed value hashing is performed $H{:}\{0,1\} * \rightarrow Z_{2^{k-1}} G{:}Z_n \rightarrow \{0,1\}^M * \ \{0,1\}^{k-1}$ for the positive integer value of M. In this public key are generated as $PK = (N, g, H, G)$.

3.1.1 Key Generation

The input obtained with the random integer k is transmitted to the escrow for signature verification. The selected integer is stated as $k - 1$ for $sk \in \left\{0, 1, \ldots, 2^{k-1} - 1\right\}$ is computed as $pk = g^{sk} mod\ N$.

3.1.2 Encryption

The process of ECC in the encryption is involved in the computation of message as $m \epsilon \{0, 1\}^m$ with the public key generation of pk for the random integer $k - 1$. The ciphertext is computed as $c = (A, B)$ with symmetric key encryption of $A = g^{H(m||r)}\ mod\ N\ and\ B = k + (m||r)$.

3.1.3 Decryption

The decryption of the encrypted data of the nodes in the MANET network is computed based on the secret key sk with the deciphering of the encrypted text as $C = \ (A, B)$ with the computation of $m\|r = B + G\left(A^{sk} mod\ N\right)$. As the proposed EsECC_SDN overall architecture of the encryption and decryption process are evaluated for analysis.

In MANET environment SDN estimated the escrow value for the estimation of the centralized environment. Upon the verification, the established trust between nodes is computed for data transmission and authentication. The computed network with SDN comprises the encryption and decryption for the classification of attacks in the network. The developed architecture process is presented in Fig. 1 and the Algorithm 1 is presented as follows.

```
Algorithm 1: Steps: Encryption with EsECC_SDN
Input: ECC points in the coordinates
Output: Generated keys H and T
These are takes within the SDN of MANET
        1. Chooses coefficients to define the elliptical curve $y^3 = x^3 + ax + b$ over finite field Fn. In
           which, a and b define the rational integers or numbers.
        2. Picks a based point $G = (x_0, y_0)$ with a large order r and this gives us $G^r = E$ (where G
           is the binary form sequence of points in the elliptical curve for ciphertext and r is the
           positive integer)
        3. Selects an integer m and m < r.
        4. Computes $B = \ G^m mod\ q$

To encrypt any message w to a particular node in MANET, SDN does the following:
        1. Randomly chooses the secret integer k in which k is the secret key generated in the SDN.
        2. Computes $H = \ G^k mod\ n$ and $T = \ B^k w\ mod\ n$ in this H is the secret key generated by the
           sender and T is computed the receiver end along with the message sequence.
        3. Produces the ciphertext (H, T).
        4. SDN has the attribute values assigned for particular node $A_1$, $A_2$, ... An.
        5. Computes $A_n\,(H, T) = \ (A_n H, A_n T\ )$
        6. Sends $(A_n H, A_n T\ )$ to node those have data.
```

(Continued)

Algorithm 1: Continued

Decryption

Input: Encryption points A_nH and A_nT

Output: Decryption of file W (file)

To decrypt the ciphertext $(A_nH, A_nT\ )$ Alice needs to do the following:

1. Computes $\mathrm{R} = \ \mathrm{A_nH^m mod\ n}$; R–Encrypted message that is transferred to the receiver node

Recovers $\mathrm{w} = \dfrac{\mathrm{A_nT}}{\mathrm{R}}\mathrm{mod\ n}$; w–Original data transmitted from the sender

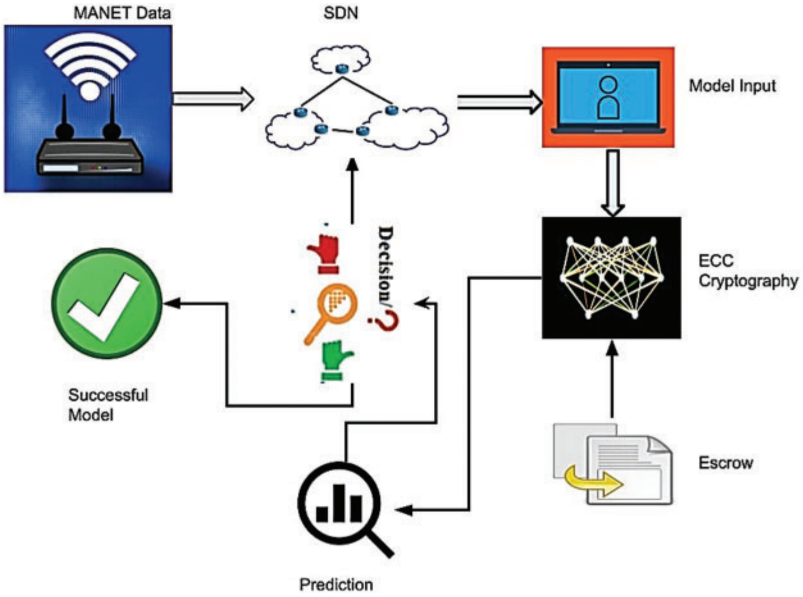

Figure 1: Overall architecture of EsECC_SDN

The public keys of the system are formed by (G, B) and can be publicly in an open channel while the private key of ECC is represented as m.The encrypted data is available at the centralized SDN, the node those wants assess to within the network needs to get permission within the network that is performed in the revocation phase. The network revocation phase comprises the deep learning techniques AdaBoost integrated regression model that classifies whether the particular node is an attacker or a normal user.

The proposed EsECC_SDN uses Add_{DH} to denote the secure addition gate, which is given the ciphertext CT_1 *and* CT_2 of plaintext kp_1 *and* kp_2 under public key pk_{DH1} *and* pk_{DH2} respectively, the calculates the sum as $c1 +_{DH} c2 = Add_{DH}(CT_1, CT_2)$. Similarly, MultiMF denotes the secure multiplication gate, the calculates the products as $CT_1 \times_{DH} CT_2 = MultiMF(CT_1, CT_2)$. Similarly, MultiMF denotes the secure multiplication gate, the calculates the products as $CT_1 \times_{DH} CT_2 = MultiMF(CT_1, CT_2)$. With the proposed EsECC_SDN transductive based HMM model is applied for the prevention and detection of attack in the MANET. As the HMM model belongs to the class of Bayesian network with computation of the probabilistics feature in the time-series analysis. The Hidden Markov model utilizes the sequences of the Hidden Markov chain in the hidden form for the computation of the different sequences randomly. In this paper the HMM is applied in the intrusion detection system for the temporal estimation of the undefined sequences in the network. The malicious within the network are computed based on the consideration of the multiple attacks with computation of the network characteristics to detect network accuracy. With estimation and identification of the temporal relationship attacks are computed and identified with consideration of the different states in the hidden layer for alerts transmits in the layer. Through application of the HMM in the malicious attack detection in the network cloud with transfer probabilities are presented in Fig. 2. The state of HMM model is denoted as s with the time instances t with the node count of n_i. The HMM model applied in the MANET network are presented in Eq. (2)

$$\lambda = (B, H, C, J, \pi) \tag{2}$$

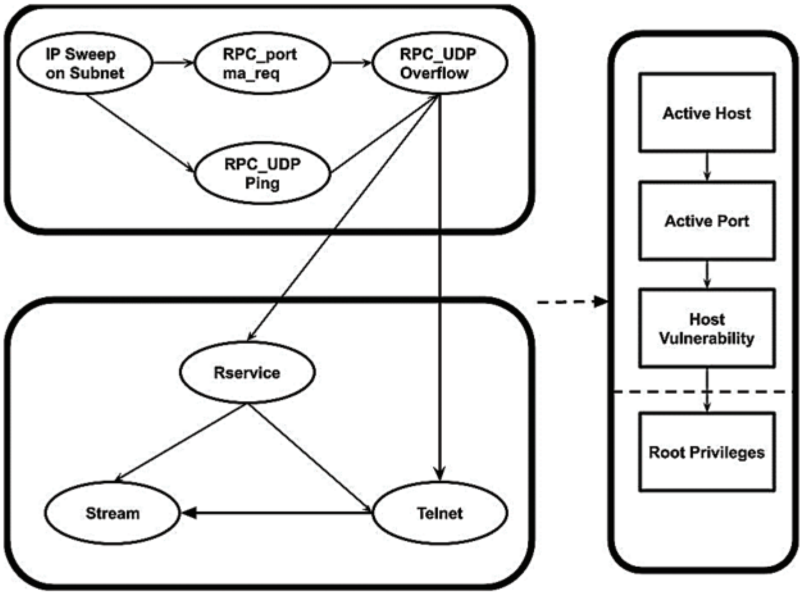

Figure 2: HMM model for attack detection

As shown in Fig. 3, the observation layer sequences are measured as $N = (n_{1,} n_2, \ldots, n_T)$ with the attack intents represented as $\mathrm{n_t = v_i}$. At some instances, the intents within the hidden layer is presented as $H\,(i_1, i_2, \ldots, i_T)$. At some times the instances can be $i_t = S_i$ based on the attack sequence conditional probability for the vertical attacks is given as $P\,(al_i|\,S_i)$. Also, with the intents with horizontal attack the conditional probability of the network scenario is defined as S_j as $P\left(S_j\middle|\,S_i\right)$. Generally, the application of HMM model comprises of the different challenges such as parameter estimation probability and decoding. The attack in the network at every stage are evaluated using transductive learning with transmission of sequence of hyper alerts with the random length of $L = (n_1, n_2, \ldots, n_M)$. In the network the positive integer value is denoted as M denoted as $N = (al_1, al_2, \ldots, al_n)$. The intents of the hidden layer attack is stated as H and the probabilistic model values are represented in Eq. (3):

$$P\,(N|\,\lambda) = \sum_I P\,(N, I|\,\lambda) = \sum_I P\,(N|\,I, \lambda)\,P\,(I|\,\lambda) \tag{3}$$

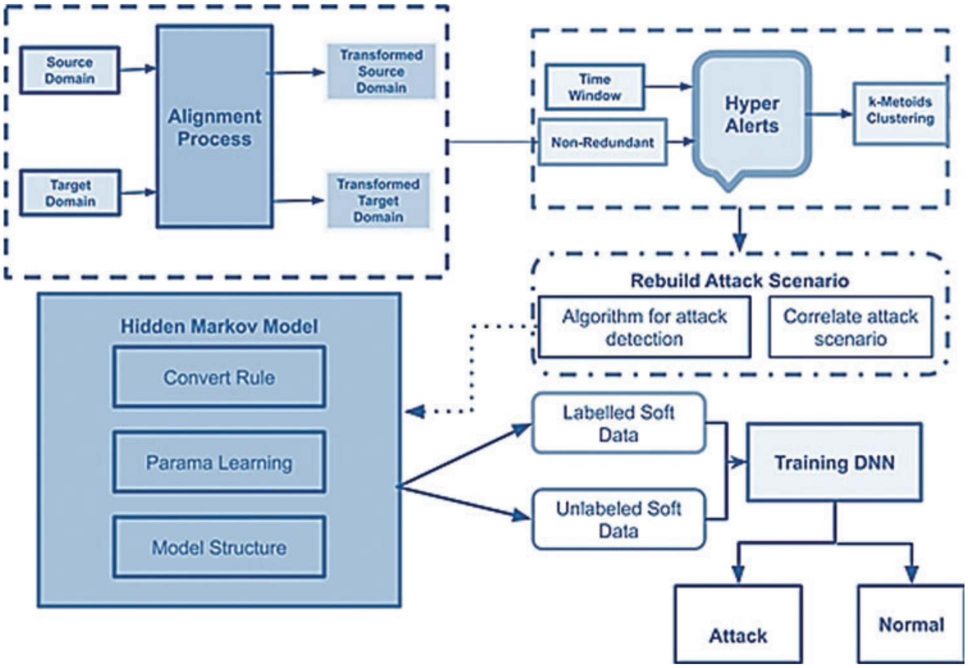

Figure 3: Overall Architecture of ESECC_SDN

To reduce the intents for each attack both forwarding and backward operation are performed. The network hidden state is denoted as t_i with the observed node $n_1, n_2, \ldots, n_t$ with the forward probability of $\alpha_t\,(i)$. For hidden state $t+1$ the corresponding state in the network is represented as $n_{t+1}, n_{t+2}, \ldots, n_T$ with the backward probability of $\beta_t\,(i)$ those are represented in the Eqs. (4) and (5).

$$\alpha_t(i) = P\left(n_1, n_2, \ldots, n_t, i_t = q_i \middle|\, \lambda\right) \tag{4}$$

$$\beta_t(i) = P\left(n_{t+1}, n_{t+2}, \ldots, n_T \middle|\, i_t = q_i, \lambda\right) \tag{5}$$

The present state of intent probability is given in Eq. (6)

$$\gamma_t\,(i) = P\left(i_t = q_i \middle|\, N, \lambda\right) = \frac{P\left(i_t = q_i,\, N \middle|\, \lambda\right)}{P\left(N \middle|\, \lambda\right)} \tag{6}$$

For backward probability, it is given in Eq. (7),

$$P\left(i_t = q_i,\, N \middle|\, \lambda\right) = \alpha_t(i)\beta_t(i) \tag{7}$$

Which provides,

$$\gamma_t\,(i) = \frac{\alpha_t(i)\beta_t(i)}{\sum_{j=1}^{N} \alpha_t(j)\beta_t(j)} \tag{8}$$

With the defined states of model λ, the observation sequence N, the probabilities are computed for each states as q_i and q_j for the time instances t and $t+1$ given in Eqs. (9)–(11)

$$\delta_t\left(i,j\right) = P\left(i_t = q_i, i_{t+1} = q_j \middle| N, \lambda\right) = \frac{P\left(i_t = q_i, i_{t+1} = q_j \middle| N, \lambda\right)}{P(N|\,\lambda)} \tag{9}$$

$$P\left(i_t = q_i, i_{t+1} = q_j,\ N|\,\lambda\right) = \alpha_t(i)a_{ij}b_j\left(N_{t+1}\right)\beta_{t+1}(j) \tag{10}$$

$$\delta_t\left(i,j\right) = \frac{\alpha_t(i)a_{ij}b_j\left(N_{t+1}\right)\beta_{t+1}(j)}{\sum_{i=1}^{N}\sum_{j=1}^{N}\alpha_t(i)a_{ij}b_j\left(N_{t+1}\right)\beta_{t+1}(j)} \tag{11}$$

The simplified form of the equation is presented in Eq. (12),

$$P\left(N|\,\lambda\right) = \sum_{i=1}^{N}\sum_{j=1}^{N}\alpha_t\left(i\right)a_{ij}b_j\left(N_{t+1}\right)\beta_{t+1}\left(j\right) \tag{12}$$

With the HM model the trained model is represented as $\lambda = (C, J, \pi)$.

3.2 Transductive Transfer Learning Framework

In second phase of the proposed ESECC_SDN architecture transfer learning with the transductive (TL) is formulated for the attack prevention. The constructed TL model involved in binary classification process for the labelled instances represented as L_s. The attack prevention can be denoted as A_s with assignment of label classes in the label cluster. With the defined technique the soft label instances are computed for the threshold values those are involved in data transfer clustering process. The labels in the TL are evaluated and derived with the HMM model values without any attack stated as λ. As stated earlier the HM model uses the attack detection and prevention denoted as $\lambda = (C, J, \pi)$. The Fig. 3 illustrates the overall architecture for the proposed ESECC_SDN model is presented.

3.2.1 Attack Prevention with ESECC_SDN

The attack prevention in the network is evaluated based on the domain capturing semantics with calculation of the HMM model ranking with consideration of the cluster group mean. The formulation of cluster is based on the consideration of the length of the cluster defined as $\left(i - 1^{th} \text{ and } i + 1^{th}\right)$ for the different domains. In the constructed cluster the similarity index is formulated as $M_s^{p,q}$. In the cluster domain p and i^{th} offers the q value of 1. Similarly, with the domain p and q for instances $(i-1)^{th}$ and $(i+1)^{th}$ the values are measured as 0.5 else it will be assigned as 0. Through source transformation domain the mapping function targeted to compute the latent space d for the different attack scenarios. Subsequently, the attack domain conversion is evaluated based on the label instances latent space for the classification of the target domain to prevent attacks. To perform attack prevention soft labelling is applied in the target instances with the appropriate training within the classifier. Through the derived HMM model the deep learning framework model uses the cluster score assignment for the attack prevention. Initially, the source cluster are assigned with labels either “normal” or “attack”. The network target domain is denoted as D_1^t and D_2^t based on source label Euclidean distance estimation and ranking as $r_i, r_i + 1, r_i - 1$, the labelling process in the HMM model is defined in sequence of steps those are listed as follows:

Step 1: Initially, all labels are stated as zero

Step 2: If ranked as r_i in the source cluster then consider the attack α is applied in the cluster else it eliminates form the cluster group

Step 3: If the source cluster ranking is provided as $r_i + 1$, with the attack $\frac{\alpha}{2}$ in the system else it will be eliminated from the group cluster.

Step 4: For ranking as $r_i - 1$ in source cluster, then attack $\frac{\alpha}{2}$ is incorporated in the cluster else it will be removed in the cluster.

Finally, the target score is computed for the estimated attacks in the instances of the cluster group. The instances threshold values T_1 provided for the soft labels of "attack" else the network T_2 considered below the threshold and considered as "normal". The instances target is defined as follows:

$T_1 = \alpha$ \\ Assign as attack

$T_2 = 1 - \alpha$ \\ Assign label as normal

In those assigned labels the instances are classified and prevented in the network with generation of the soft labels. Within the cluster group the labels are assigned based consideration of different attack parts to perform classification. The cluster within the node are evaluated based on consideration of different factors such as conditional probability table (CPT), prior knowledge and edge probability. Through the causality the attacks are estimated in the HMM model with the transductive transfer learning. Hence, the unknown attack label instances are estimated and updated as given in Eq. (13)

$$U_{ij}^{t} = \begin{cases} \delta + (1-\delta)\,U_{ij}^{t-1}, & P\left(u_i \middle| y_t\right) = 1 \quad P\left(u_j \middle| y_t\right) = 1 \\ (1-\delta)\,U_{ij}^{t-1}, & P\left(u_i \middle| y_t\right) = 1 \quad P\left(u_j \middle| y_t\right) = 0 \\ \mathrm{U}_{\mathrm{ij}}^{\mathrm{t-1}} & \text{otherwise} \end{cases} \tag{13}$$

Based on the assigned label instances for the unknown attack T_1 and T_2 instances with the CPT are denoted as $U_{ij} = P\left(X = x_j \middle| U = u_i\right)$. In Fig. 4 the overall architecture process involved in proposed ESECC_SDN is presented for attack prevention and detection. The attack detected with the HMM model comprises of the transductive network model for the attack training and computational process.

In the dataset the assigned label is evaluated with the elimination of the attacks represented as $D\,(D = \{y_1, y_2, y_3, \ldots\})$ through elimination of the data attack y_t. The attack scenario in the HMM model is stated as $S = (I_1, I_2, \ldots, I_n)$. The Algorithm 2 provides the estimation of attack scenario in the network is presented below.

Algorithm 2: Parameter Estimation

```
Input: Sequence of attack in network = $\{(al_1, al_2 \ldots)\ (al_3, al_4 \ldots) \ldots\}$
Output: $\delta^{n+1} = \left(C^{n+1}, J^{n+1}, \lambda^{n+1}\right)$
// Start
For n = 0 generate $\delta_i^0$
For $a_{ij}^0 = \delta_i^0$ set $b_j(k)^0$
For unknown attack n = 0, 1, 2 . . .
  do
Calculate using Eq. (11)
Calculate using Eq. (12)
```

(Continued)

Algorithm 2: Continued

```
    End for
  End for
Set values
Set comparison value
    If $P(Z_i = 1 | I_i = 1) > trustValue$
      then
Compare $T_1$ and $T_2$ with estimated value
    End if
      for $value(Z_i)$ compare attack value
        If $value(Z_i) > trustValue$ then
        Compute new set $Z_i$
        End if
      End for
    End for
```

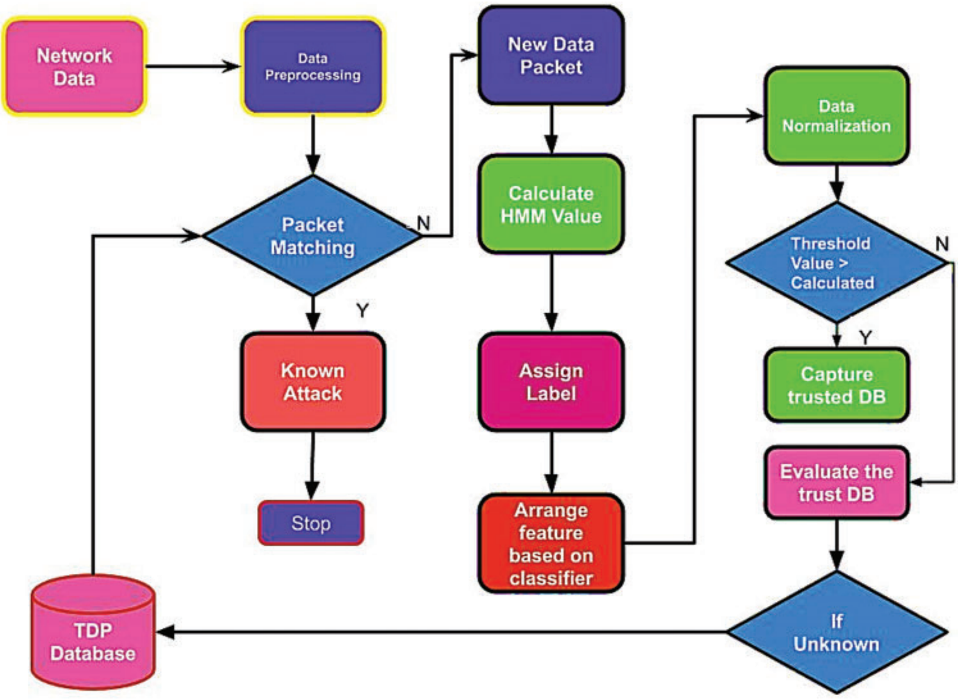

Figure 4: Overall Flow of ESECC_SDN

In transductive model the source mapping is generated for the targeted source with computation of the latent space in the domain. Through the conversion of the latent space the labels are assigned to the attack classifier. The soft label assignment provides the data accuracy process for the classifier training in the instances of the target. The assignment of the attack estimation is presented in Algorithm 3 for the prevention and classification.

The HMM based attack estimation computes the attack instances in the network through the calculated threshold values with the threshold label assignment and construction of the parameters.

The developed model uses the transductive deep learning model for the training in which the attack are characterized as A_{attack} and network real data is represented as D. In real-time data the training sequences are defined as $D(S(z))$ for the transductive layer value of 1. The maximization process in the transductive learning is given as $V(S, D)$ for the trained data D in the layer S. Similarly, with the minimization of the second order training in data $D(S(z))$ the attack prevention and detection is evaluated using $V(S, D)$ as $\underset{S}{min}\,\underset{D}{max}\, V(D, S) = E_x - A_{attack(x)}[\log D(x)] + E_{z-p_z(Z)}[\log(1 - D(S(z)))$. The distributed data convergence is denoted as $V\ (D,\ S)$ with the detection of attack in transductive learning process is computed as $\left(Z_{ij}\right)$. The convergence in data is presented in Eq. (14).

$$Z_{ij} = \sum_{a=0}^{m-1} \sum_{b=0}^{m-1} w_{ij} x_{ij} \tag{14}$$

In the TDL system the attacks are computed as presented in Eqs. (15) and (16)

$$\underset{S}{min}\, log\,(1 - D(S(Z))) \tag{15}$$

$$\Leftrightarrow D(S(Z)) \approx 1 \tag{16}$$

$$\Leftrightarrow S(z) \approx x \in \chi;$$

In above condition the χ represets the dataset in real-time scenario. The training process in the HMM-TDL is given in Eq. (17) as follows:

$$P(D^*, S^*) \le P(D^*, S)\, \forall S \tag{17}$$

With incorporated HMM model with transductive deep learning attack is detection and those are subjected to constraints represented as in Eqs. (18)–(28)

Case 1: If $A_{attack} \approx A_s$ data used in the training process xConsider $P(D^*,\ S^*)$ for the minimal data value of $A_{attack}(x) \le A_s(x)$

This will be $A_{attack}(x) \le A^*{}_S(x)$

$$P(D^*, S) = \int_x A_{attack}(x)\, D^*(x)\, dx + \int_x A_{data}(x)\, D^*(S(z))\, dz \tag{18}$$

$$= \int_x A_{attack}(x)\, D^*(x) + A_S(x)\,(1 - D^*(x))\, dx \tag{19}$$

$$= \int_x A_{attack}(x)\, D^*(x) - p_S(x)\, dx + \int_x p_s(x)\, dx \tag{20}$$

$$= \int_x 1 A_{attack}(x) > A_s(x)\,(A_{attack}(x) - A_s(x))\, dx + \int_x A_s(x)\, dx \tag{21}$$

$$\ge \int_x A_S(x)\, dx \tag{22}$$

Case 2: Consider $P(D^*,\ S^*)$ as minimal value for data

$A_{attack}(x) \ge A_s(x)$

This will be $A_{attack}(x) \geq A^{*}{}_{S}(x)$

$$P(D^{*}, S) = \int_{x} A_{attack}(x)\,(1 - D(x)\,dx + \int_{x} A_{data}(x)\,D(S^{*}(z))\,dz \tag{23}$$

$$= \int_{x} A_{attack}(x)\,(1 - D(x))\,dx + \int_{x} A_{S}(x)\,(D(x))\,dx \tag{24}$$

$$= \int_{x} D(x) - (p_{G^{*}}(x) - p_{data}(x))\,dx + \int_{x} p_{data}(x)\,dx \tag{25}$$

$$= \int_{x} 1A_{attack}(x) > A_{G^{*}}(x)\,(A_{G^{*}}(x) - A_{data}(x))\,dx + \int_{x} A_{data}(x)\,dx \tag{26}$$

Algorithm 3: Attack Estimation parameters

```
Input: Compute the target domain
Output: Assign the label for the attacks for the latent space in d-dimensions
    Construct the data node matrix $Z = \begin{pmatrix} X_1 & 0\ldots & 0 \\ \ldots & \ldots & \ldots \\ 0\ldots & 0 & X_k \end{pmatrix}$
    1. Compute matrix $W_k$ for estimation of node distances as $W_k(i.j) = e^{-||-x_i - x_j||^2}$
    2. Compute similarity indices in the matrix using Laplacian transformation $L_x = D_x - W_x$
    3. Compute the attack node using Laplacian matrix for attack computation $L = \begin{pmatrix} L_1 & 0\ldots & 0 \\ \ldots & \ldots & \ldots \\ 0\ldots & 0 & L_k \end{pmatrix}$
    4. Compute eigen vector dimensionality with mapping function $Z(\delta L + L_s)\,Z^T x = \delta Z L_d Z^T x$
    5. Transform latent dimension of data as the target domain
```

$$\geq \int_{x} 1A_{data}(x) > A_{G^{*}}(x)\,(A_{data}(x))\,dx \tag{27}$$

$$\geq -M \tag{28}$$

3.3 Dataset Description

The proposed EsECC_SDN concentrated on the attack classification mechanism for MANET environment. To estimate the attack detection and classification this paper uses CICICS 2020 dataset. The SDN mechanism focused on the attack classification and detection rate of the network. The proposed scheme uses the SVM classification model for attack detection. However, for efficient processing of data optimal subset features need to be processed with the elimination of irrelevant features without impact on the computational cost and accuracy. The attack classification model for MANET is presented in Fig. 5. The developed EsECC_SDN uses the CICIDS dataset for training and testing the attack. Based on the attributes of the given dataset, attacks in the MANET are computed for training and testing of the attack sequences. The separation of the dataset for training and testing is presented in Tab. 2.

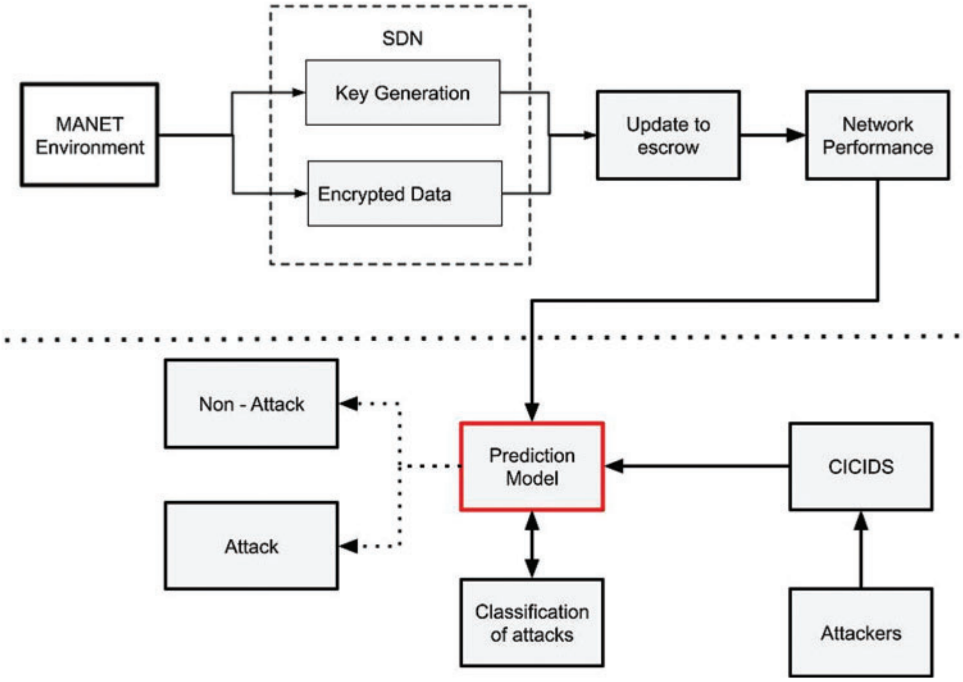

Figure 5: EsECC_SDN attack classification Model

Table 2: Dataset distribution

	Data distribution	Training count	Testing count
Attack distribution	Normal activity	67,343	9,710
	Anomaly	58,630	12,834
	DoS	45,927	7,458
	Probe attack	11,656	2,422
	U2R (User to root) attack	52	67
	R2L (Root to local)	995	2,887
	Black hole attack	12,945	999

With the distribution of training and testing of the dataset, attacks are computed in the MANET network. The training of data comprises 70% of data for training to achieve the desired accuracy with the remaining data is utilized for testing the performance of the network.

4 Simulation Results

The performance of the proposed EsECC_SDN is implemented in Network Simulator [3] attack detection and prevention in the MANET environment. Tab. 3 presents the simulation setting for the proposed EsECC_SDN. With SDN centralized architecture performance characteristics of EsECC_SDN are evaluated. The simulation is computed under two scenarios such as:

- A varying number of nodes
- Attackers Scenario

Table 3: Simulation setting

Simulation parameters	Values
Simulation software	Phython
Mobility of node	4 (ms/s), 6 (ms/s) and 10 (ms/s)
No.of nodes	10, 20, 30, 40, and 50
Channel	Multi-path

The performance characteristics of the proposed EsECC_SDN with the different parameters are computed those are Delay, Jitter, End-to-End delay, Packet Delivery Rate (PDR) and Throughput.

The performance of the proposed ESECC_SDN scheme performance is computed based on the varying mobility of nodes. The mobility of nodes is varied with respect to 4, 6 and 10 (ms/s). Similarly, for varying the mobility number of nodes are varied as 10, 20, 30, 40, and 50. Tab. 4 presented the performance of the network for varying mobility of nodes.The performance of the proposed EsECC_SDN is comparatively examined with the existing technique such as Dynamic Source Routing (DSR) [19], Three-Dimensional Clustered (TDC) [20] and Artificial Danger Theory (ADT) [17]. The performance of the proposed EsECC_SDN architecture involved in encryption and decryption of MANET data for analysis. The comparison of the performance is estimated based on the varying number of nodes and the attack nodes in the MANET environment.

Table 4: Performance computation of MANET without attackers

		Delay (s)		
No.of nodes	DSR [19]	Three-dimensional clustering (TDC) [20]	Artificial danger theory (ADT) [17]	EsECC_SDN proposed
10	21	18	16	8
20	27	21	20	10
30	34	26	24	13
40	39	29	28	16
50	43	32	31	19
		Loss %		
No.of nodes	DSR [19]	Three-dimensional clustering (TDC) [20]	Artificial danger theory (ADT) [17]	EsECC_SDN proposed
10	33	28	21	10
20	38	31	26	13
30	42	34	29	19
40	46	38	32	23
50	52	42	36	27

(Continued)

Table 4: Continued

PDR %				
No.of nodes	DSR [19]	Three-dimensional clustering (TDC) [20]	Artificial danger theory (ADT) [17]	EsECC_SDN proposed
10	43	58	73	99
20	40	52	69	98
30	37	48	67	97
40	34	43	64	97
50	29	38	63	96
Control Overhead				
No.of nodes	DSR [19]	Three-dimensional clustering (TDC) [20]	Artificial danger theory (ADT) [17]	Esecc_SDN proposed
10	21.89	10.67	4.78	1.49
20	19.73	9.75	5.34	1.64
30	16.57	8.56	5.89	1.93
40	13.47	8.45	6.35	2.34
50	10.56	7.89	7.50	2.96
Throughput (kbps)				
No.of nodes	DSR [19]	Three-dimensional clustering (TDC) [20]	Artificial danger theory (ADT) [17]	EsECC_SDN proposed
10	43	51	59	63
20	39	48	55	60
30	36	46	53	58
40	33	43	48	55
50	28	41	44	51

Fig. 6 shows the delay of the proposed EsECC_SDN compared with the DSR, TDC, and ADT. Simulation results show that the proposed method gives a minimum delay when the node count is from 10 to 50 nodes.

Fig. 7 shows the loss of the proposed EsECC_SDN compared with the DSR, TDC, and ADT. Simulation results show that the proposed method gives a minimum loss when the node count is from 10 to 50 nodes. Fig. 8 shows the packet delivery ratio of the proposed EsECC_SDN compared with the DSR, TDC, and ADT. Simulation results show that the proposed method gives a maximum packet delivery ratio when the node count is from 10 to 50 nodes.

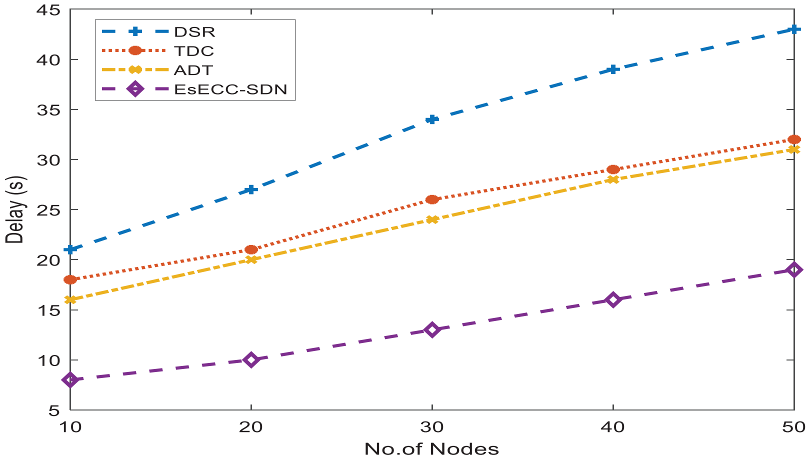

Figure 6: Comparison of delay

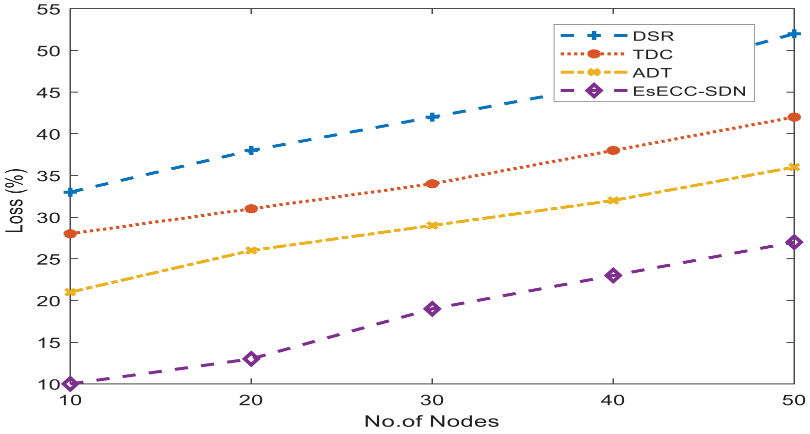

Figure 7: Comparison of loss

Fig. 9 shows the control overhead of the proposed EsECC_SDN compared with the DSR, TDC, and ADT. Simulation results show that the proposed method required a minimum overhead when the node count is from 10 to 50 nodes. Fig. 10 shows the throughput of the proposed EsECC_SDN compared with the DSR, TDC, and ADT. Simulation results show that the proposed method gives a maximum throughput when the node count is from 10 to 50 nodes. The performance of the proposed EsECC_SDN expressed that with an increase in the number of nodes loss and delay is increases. Furthermore, the PDR and throughput of the MANET network are reduced compared with existing techniques.

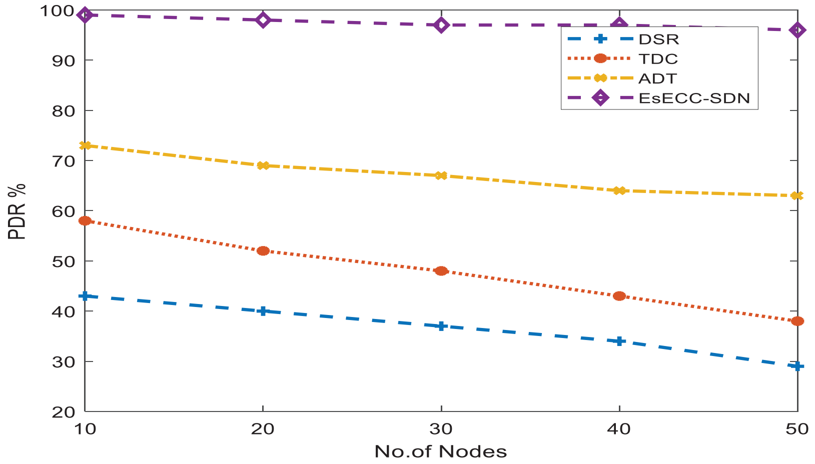

Figure 8: Comparison of PDR

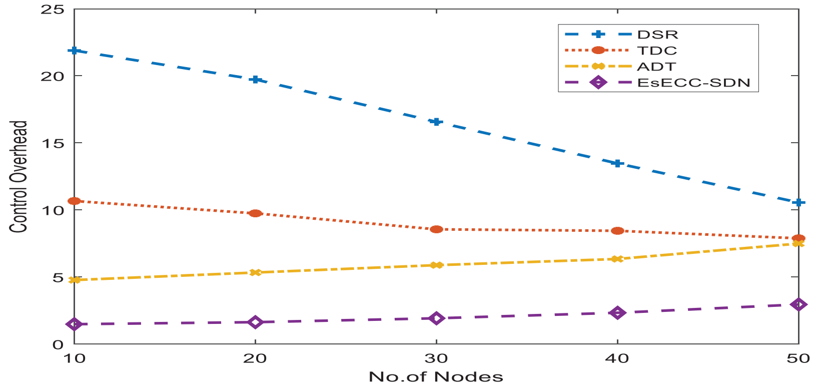

Figure 9: Comparison of control overhead

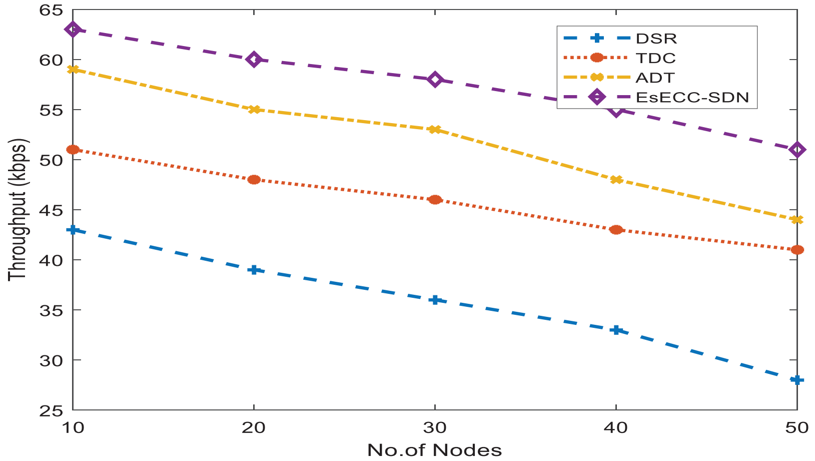

Figure 10: Comparison of throughput

The performance of the proposed EsECC_SDN is significant exhibits minimal delay and loss. Moreover, the network PDR and throughput are higher but with the increase in the number of nodes is reduced. In addition, the mobility of nodes does not have a significant impact on the MANET performance. The proposed EsECC_SDN is involved in the classification of attacks in the network. The analysis is based on the consideration of the CICIDS dataset for attack classification and detection is shown in Fig. 11. The model performance is classified based on the SVM classifier. As the proposed EsECC_SDN is involved in the detection of attacks in the MANET network. Based on the training data, attacks are classified in the network for consideration of different attacker's environments. The comparative analysis of results obtained for MANET with and without attackers' environment expressed that with attacker's environment the performance is significantly reduced. The performance of the proposed EsECC_SDN for attack classification is presented in Tab. 5.

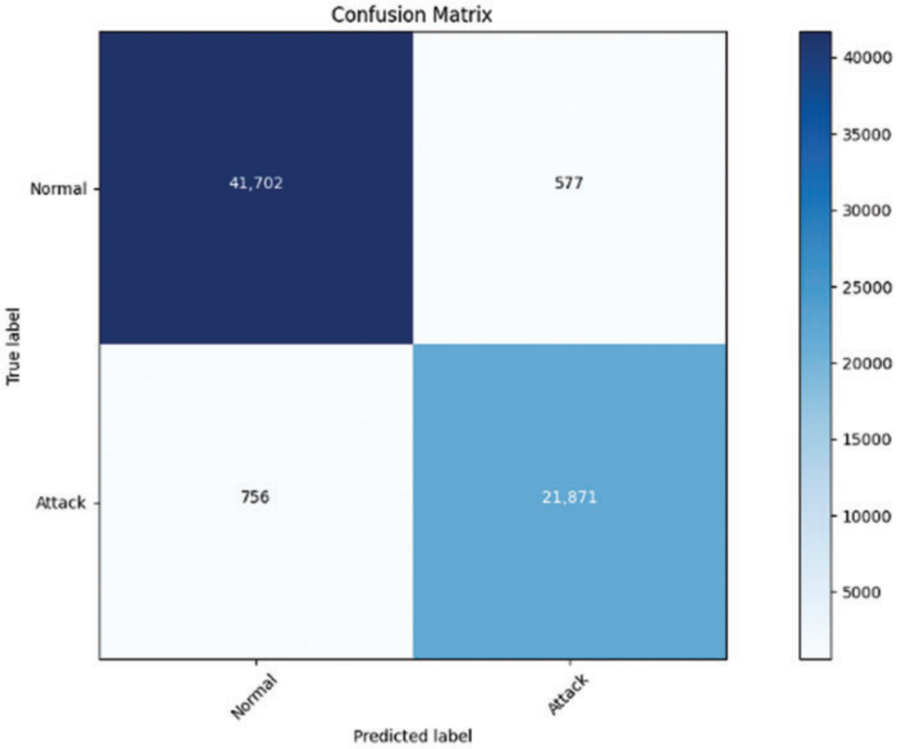

Figure 11: Confusion matrix for NSL-KDD dataset

Table 5: EsECC_SDN attack classification performance

	Accuracy	Precision	Recall
Normal activity	97	97	98
Anomaly	98	97	98
DoS	95	96	96
Probe Attack	91	91	92

(Continued)

Table 5: Continued

	Accuracy	Precision	Recall
U2R (User to root) attack	91	92	91
R2L (Root to local)	94	95	95
Black hole attack	96	96	95

The proposed EsECC_SDN scheme classifier performance for different attacks is computed for analysis. The analysis expressed that the proposed EsECC_SDN scheme exhibits a higher accuracy value of anomaly with 98%. In the case of a black hole attack, the classification accuracy is estimated as 96%. Similarly, in the estimation of precision DoS and Blackn hole attack, it is achieved as 96%. The recall value is estimated higher value of 98% for anomaly detection. The comparative analysis of the propised EsECC_SDN with the model is included in the accuracy with the consideration of the different attack scenario. The accuracy of the classification is computed as 97% for the normal activity, anomaly as 98%, DoS as 95%, Probe atatck as 91%, U2R as 91%, R2L is 94% and black hole attack as 96%. In Tab. 6, the attack classification performance of the proposed EsECC_SDN with conventional classifiers such as AdaBoost, ANN, and ensemble classifier is presented.

Table 6: Comparative analysis of classifier

Parameters	AdaBoost	ANN	Ensemble classifier	Proposed EsECC_SDN
Accuracy %	93	94	95	98
Precision %	92	92	96	97
Recall %	91	91	91	97
F1–score	0.923	0.936	0.93	0.965

The attack classification performance expressed that the proposed EsECC_SDN scheme achieves an accuracy of 98% while AdaBoost, ANN, and ensemble exhibit the accuracy of 97%, 96%, and 97% respectively. This implies that the proposed EsECC_SDN scheme exhibits significant performance in attacks classification. Similarly, in the case of recall proposed EsECC_SDN achieves a higher percentage rather than AdaBoost, ANN, and ensemble classifiers. The recall of the proposed EsECC_SDN is 97%, which is approximately 3% higher than the conventional technique AdaBoost, ANN, and ensemble classifier

5 Conclusion

MANET network subjected to vast range of security issues and challenges due to presence of higher node mobility scenario. This paper is presented a security scheme for the MANET network for attack prevention and classification using SDN architecture. The proposed EsECC_SDN scheme uses the data encryption and decryption using ECC scheme within the SDN network. In next stage, the attacks are prevented and detected using the model with transductive learning with computation of k-centroids with hyper alerts. The performance of the proposed EsECC_SDN evaluated for the attack detection and classification. The classification of the EsECC_SDN model uses the classifier for the classification of attacks. The proposed model achieves the overall accuracy of 98% for the cryptography-based scheme in SDN model. The comparative analysis of the proposed EsECC_SDN with the conventional AdaBoost, ANN, and ensemble classifier exhibits improved performance for attack classification. Through analysis, it can be concluded that the proposed EsECC_SDN scheme is effective for secure data transmission in the MANET network. In the future, this work can be improved in a real-time attack detection scheme in an Intrusion Detection System (IDS).

Acknowledgement: The authors would like to thank the Deanship of Scientific Research at Umm Al-Qura University for supporting this work by Grant Code: (22UQU4281768DSR05).

Funding Statement: Deanship of Scientific Research at Umm Al-Qura University, Grant Code, funds this research: 22UQU4281768DSR05.

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

References

[1] K. N. Dattatraya and K. Raghava Rao, “Hybrid based cluster head selection for maximizing network lifetime and energy efficiency in WSN,” *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 3, pp. 716–726, 2022.

[2] N. V. Patil, C. R. Krishna, K. Kumar and S. Behal, “E-Had: A distributed and collaborative detection framework for early detection of DDoS attacks,” *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 4, pp. 1373–1387, 2022.

[3] N. Veeraiah and B. T. Krishna, “Trust-aware FuzzyClus-fuzzy NB: Intrusion detection scheme based on fuzzy clustering and Bayesian rule,” *Wireless Networks*, vol. 25, pp. 4021–4035, 2019.

[4] M. S. Shaik and F. Mira, “A comprehensive mechanism of manet network layer based security attack prevention,” *International Journal of Wireless and Microwave Technologies*, vol. 10, no. 1, pp. 38–47, 2020.

[5] Y. Alotaibi, M. N. Malik, H. H. Khan, A. Batool, S. ul Islam *et al.,* “Suggestion mining from opinionated text of big social media data,” *Computers, Materials & Continua*, vol. 68, no. 3, pp. 3323–3338, 2021.

[6] N. Veeraiah and B. T. Krishna, “An approach for optimal-secure multi-path routing and intrusion detection in MANET,” *Evolutionary Intelligence*, vol. 15, pp. 1313–1327, 2020.

[7] N. Veeraiah and B. T. Krishna, “Intrusion detection based on piecewise fuzzy C-means clustering and fuzzy naïve Bayes rule,” *Multimedia Research*, vol. 1, no. 1, pp. 27–32. 2018.

[8] P. Bellavista, C. Giannelli, L. Thomas and S. Panagiotis, “Multi-domain SDN controller federation in hybrid FiWi-MANET networks,” *EURASIP Journal on Wireless Communications and Networking*, vol. 1, pp. 1–19, 2018.

[9] J. Maruthupandi, S. Prasanna, P. Jayalakshmi, V. Mareeswari and B. Siva Kumar, “Route manipulation aware software-defined networks for effective routing in SDN controlled MANET by disney routing protocol,” *Microprocessors and Microsystems*, vol. 80, pp. 103401, 2021.

[10] P. Bellavista, A. Dolci and C. Giannelli, “MANET-Oriented SDN: Motivations, challenges, and a solution prototype,” in *2018 IEEE 19th Int. Symp. on “A World of Wireless, Mobile and Multimedia Networks” (WoWMoM)*, Chania, Greece, pp. 14–22, 2018.

[11] H. C. Yu, G. Quer and R. R. Rao, “Wireless SDN mobile ad hoc network: From theory to practice,” in *Proc. IEEE Int. Conf. on Communications (ICC)*, Paris, France, pp. 1–7, 2017.

[12] P. Ranjit and B. Samarjeet, “A detailed analysis of CICIDS2017 dataset for designing intrusion detection systems,” *International Journal of Engineering & Technology*, vol. 7, pp. 479–482, 2018.

[13] D. Gautam, and V. Tokekar, “A novel approach for detecting DDoS attack in MANET,” *Materials Today: Proceedings*, vol. 29, pp. 674–677, 2020.

[14] V. Alappatt and P. J. Prathap, “Hybrid cryptographic algorithm based key management scheme in MANET,” *Materials Today: Proceedings*, 2020.

[15] B. Yang, Z. Wu, Y. Shen, X. Jiang and S. Shen, “On delay performance study for cooperative multicast MANETs,” *Ad Hoc Networks*, vol. 102, pp. 102–117, 2020.

[16] E. Elmahdi, S. M. Yoo and S. Kumar, “Secure and reliable data forwarding using homomorphic encryption against blackhole attacks in mobile ad hoc networks,” *Journal of Information Security and Applications*, vol. 51, pp. 102425, 2020.

[17] S. A. Syed, “A systematic comparison of mobile Ad-hoc network security attacks,” *Materials Today: Proceedings*, 2021.

[18] L. E. Jim, N. Islam and M. A. Gregory, “Enhanced MANET security using artificial immune system based danger theory to detect selfish nodes,” *Computers & Security*, vol. 113, pp. 102538, 2022.

[19] N. C. Singh and A. Sharma, “Resilience of mobile ad hoc networks to security attacks and optimization of routing process,” *Materials Today: Proceedings*, 2020.

[20] T. Ramya, J. M. Mathana, R. Nirmala and R. Gomathi, “Exploration on enhanced quality of services for MANET through modified lumer and Fai-eta algorithm with modified AODV and DSR protocol,” *Materials Today: Proceedings*, 2021.

[21] A. Tahir, N. Shah, S. A. Abid, W. Z. Khan and A. K. Bashir, “A three-dimensional clustered peer-to-peer overlay protocol for mobile ad hoc networks,” *Computers & Electrical Engineering*, vol. 94, pp. 107364201, 2021.

[22] P. Mohan, N. Subramani, Y. Alotaibi, S. Alghamdi, O. I. Khalaf *et al.,* “Improved metaheuristics-based clustering with multihop routing protocol for underwater wireless sensor networks,” *Sensors*, vol. 22, no. 4, pp. 1618, 2022.

[23] A. Thakkar and R. Lohiya, “A review of the advancement in intrusion detection datasets,” *Procedia Computer Science*, vol. 167, pp. 636–645, 2020.

[24] R. Rout, P. Parida, Y. Alotaibi, S. Alghamdi and O. I. Khalaf, “Skin lesion extraction using multiscale morphological local variance reconstruction based watershed transform and fast fuzzy C-means clustering,” *Symmetry*, vol. 13, no. 11, pp. 2085, 2021.

[25] N. Subramani, P. Mohan, Y. Alotaibi, S. Alghamdi and O. I. Khalaf, “An efficient metaheuristic-based clustering with routing protocol for underwater wireless sensor networks,” *Sensors*, vol. 22, pp. 415, 2022.

[26] S. Rajendran, O. I. Khalaf, Y. Alotaibi and S. Alghamdi, “MapReduce-based big data classification model using feature subset selection and hyperparameter tuned deep belief network,” *Scientific Reports*, vol. 11, no. 1, pp. 1–10, 2021.

[27] U. Srilakshmi, N. Veeraiah, Y. Alotaibi, S. A. Alghamdi, O. I. Khalaf *et al.,* “An improved hybrid secure multipath routing protocol for MANET,” *IEEE Access*, vol. 9, pp. 163043–163053, 2021.

[28] A. Alsufyani, Y. Alotaibi, A. O. Almagrabi, S. A. Alghamdi and N. Alsufyani, “Optimized intelligent data management framework for a cyber-physical system for computational applications,” *Complex & Intelligent Systems*, pp. 1–13, 2021.

[29] S. Bharany, S. Sharma, S. Badotra, O. I. Khalaf, Y. Alotaibi *et al.,* “Energy-efficient clustering scheme for flying ad-hoc networks using an optimized LEACH protocol,” *Energies*, vol. 14, no. 19, pp. 6016, 2021.

[30] N. Veeraiah, O. I. Khalaf, C. V. P. R. Prasad, Y. Alotaibi, A. Alsufyani *et al., “*Trust aware secure energy efficient hybrid protocol for manet,” *IEEE Access*, vol. 9, pp. 120996–121005, 2021.

[31] Y. Alotaibi, “A new database intrusion detection approach based on hybrid meta-heuristics,” *Computers, Materials & Continua*, vol. 66, no. 2, pp. 1879–1895, 2021.

[32] Y. Alotaibi, “A new secured E-government efficiency model for sustainable services provision,” *Journal of Information Security and Cybercrimes Research*, vol. 3, no. 1, pp. 75–96, 2020.

[33] V. Ramasamy, Y. Alotaibi, O. I. Khalaf, P. Samui and J. Jayabalan, “Prediction of groundwater table for chennai region using soft computing techniques,” *Arabian Journal of Geosciences*, vol. 15, no. 9, pp. 1–19, 2022.

[34] D. Anuradha, N. Subramani, O. I. Khalaf, Y. Alotaibi, S. Alghamdi *et al.,* “Chaotic search-and-rescue-optimization-based multi-hop data transmission protocol for underwater wireless sensor networks,” *Sensors*, vol. 22, no. 8, pp. 2867, 2022.

[35] Y. Alotaibi, “A new meta-heuristics data clustering algorithm based on tabu search and adaptive search memory,” *Symmetry*, vol. 14, no. 3, pp. 623, 2022.

[36] J. Jayapradha, M. Prakash, Y. Alotaibi, O. I. Khalaf and S. A. Alghamdi, “Heap bucketization anonymity-an efficient privacy-preserving data publishing model for multiple sensitive attributes,” *IEEE Access*, vol. 10, pp. 28773–28791, 2022.

[37] S. S. Rawat, S. Alghamdi, G. Kumar, Y. Alotaibi, O. I. Khalaf *et al.,* “Infrared small target detection based on partial sum minimization and total variation,” *Mathematics*, vol. 10, pp. 671, 2022.

[38] Y. Alotaibi and A. F. Subahi, “New goal-oriented requirements extraction framework for e-health services: A case study of diagnostic testing during the COVID-19 outbreak,” *Business Process Management Journal*, vol. 28, no. 1, pp. 273–292, 2022.

[39] G. Suryanarayana, K. Chandran, O. I. Khalaf, Y. Alotaibi, A. Alsufyani *et al.,* “Accurate magnetic resonance image super-resolution using deep networks and Gaussian filtering in the stationary wavelet domain,” *IEEE Access*, vol. 9, pp. 71406–71417, 2021.

[40] G. Li, F. Liu, A. Sharma, O. I. Khalaf, Y. Alotaibi *et al.,* “Research on the natural language recognition method based on cluster analysis using neural network,” *Mathematical Problems in Engineering*, vol. 2021, pp. 13, 2021.

[41] N. Jha, D. Prashar, O. I. Khalaf, Y. Alotaibi, A. Alsufyani *et al.,* “Blockchain based crop insurance: A decentralized insurance system for modernization of Indian farmers,” *Sustainability*, vol. 13, no. 16, pp. 8921, 2021.

[42] A. F. Subahi, Y. Alotaibi, O. I. Khalaf and F. Ajesh, “Packet drop battling mechanism for energy aware detection in wireless networks,” *Computers, Materials & Continua*, vol. 66, no. 2, pp. 2077–2086, 2021.

[43] H. H. Khan, M. N. Malik, R. Zafar, F. A. Goni, A. G. Chofreh *et al.,* “Challenges for sustainable smart city development: A conceptual framework,” *Sustainable Development*, vol. 28, no. 5, pp. 1507–1518, 2020.

[44] N. Veeraiah and B. T. Krishna, “Selfish node detection IDSM based approach using individual master cluster node,” in *2018 2nd Int. Conf. on Inventive Systems and Control (ICISC)*, Coimbatore, India, pp. 427–431, 2018.

[45] A. Sundas, S. Badotra, Y. Alotaibi, S. Alghamdi and O. I. Khalaf, “Modified bat algorithm for optimal vm’s in cloud computing,” *Computers, Materials & Continua*, vol. 72, no. 2, pp. 2877–2894, 2022.

[46] S. Sennan, K. Gopalan, Y. Alotaibi, D. Pandey and S. Alghamdi, “EACR-LEACH: Energy-aware cluster-based routing protocol for WSN based IoT,” *Computers, Materials & Continua*, vol. 72, no. 2, pp. 2159–2174, 2022.

[47] S. R. Akhila, Y. Alotaibi, O. I. Khalaf and S. Alghamdi, “Authentication and resource allocation strategies during handoff for 5G IoVs using deep learning,” *Energies*, vol. 15, no. 6, pp. 2006, 2022.

[48] P. Kollapudi, S. Alghamdi, N. Veeraiah, Y. Alotaibi, S. Thotakura *et al.,* “A new method for scene classification from the remote sensing images,” *Computers, Materials & Continua*, vol. 72, no. 1, pp. 1339–1355, 2022.

[49] U. Srilakshmi, S. Alghamdi, V. V. Ankalu, N. Veeraiah and Y. Alotaibi, “A secure optimization routing algorithm for mobile ad hoc networks,” *IEEE Access*, vol. 10, pp. 14260–14269, 2022.

[50] S. Palanisamy, B. Thangaraju, O. I. Khalaf, Y. Alotaibi and S. Alghamdi, “Design and synthesis of multi-mode bandpass filter for wireless applications,” *Electronics*, vol. 10, pp. 2853, 2021.

[51] S. Sennan, D. Pandey, Y. Alotaibi and S. Alghamdi, “A novel convolutional neural networks based spinach classification and recognition system,” *Computers, Materials & Continua*, vol. 73, no. 1, pp. 343–361, 2022.

[52] A. R. Khaparde, F. Alassery, A. Kumar, Y. Alotaibi, O. I. Khalaf *et al.,* “Differential evolution algorithm with hierarchical fair competition model,” *Intelligent Automation & Soft Computing*, vol. 33, no. 2, pp. 1045–1062, 2022.

[53] H. H. Khan, M. N. Malik, Y. Alotaibi, A. Alsufyani and S. Alghamdi, “Crowdsourced requirements engineering challenges and solutions: A software industry perspective,” *Computer Systems Science and Engineering*, vol. 39, no. 2, pp. 221–236, 2021.