An effective communication and computation model based on a hybridgraph-deeplearning approach for SIoT.

MEKALA, M.S., SRIVASTAVA, G., PARK, J.H. and JUNG, H.-Y.

2022

Digital Communications and Networks 8 (2022) 900–910

Contents lists available at ScienceDirect

Digital Communications and Networks

journal homepage: www.keaipublishing.com/dcan

An effective communication and computation model based on a hybridgraph-deeplearning approach for SIoT

M.S. Mekala [a,b], Gautam Srivastava [c,e], Ju H. Park [d], Ho-Youl Jung [a,*]

[a] Department of Information and Communication Engineering, Yeungnam University, Gyeongsan, 38544, South Korea
[b] RLRC LAb for Autonomous Vehicle Parts and Materials Innovation, Yeungnam University, Gyeongsan, 38544, South Korea
[c] Department of Math and Computer Science, Brandon University, Brandon, Canada
[d] Department of Electrical Engineering, Yeungnam University, Gyeongsan, South Korea
[e] Research Centre for Interneural Computing, China Medical University, Taichung, Taiwan, China

ARTICLE INFO

Keywords:
Edge computing
Adaptive trust weight (ATW) model
Quotient user-centric coeval-learning (QUCL) mechanism
Deep learning
Service reliability

ABSTRACT

Social Edge Service (SES) is an emerging mechanism in the Social Internet of Things (SIoT) orchestration for effective user-centric reliable communication and computation. The services are affected by active and/or passive attacks such as replay attacks, message tampering because of sharing the same spectrum, as well as inadequate trust measurement methods among intelligent devices (roadside units, mobile edge devices, servers) during computing and content-sharing. These issues lead to computation and communication overhead of servers and computation nodes. To address this issue, we propose the HybridgrAph-Deep-learning (HAD) approach in two stages for secure communication and computation. First, the Adaptive Trust Weight (ATW) model with relation-based feedback fusion analysis to estimate the fitness-priority of every node based on directed graph theory to detect malicious nodes and reduce computation and communication overhead. Second, a Quotient User-centric Coeval-Learning (QUCL) mechanism to formulate secure channel selection, and Nash equilibrium method for optimizing the communication to share data over edge devices. The simulation results confirm that our proposed approach has achieved effective communication and computation performance, and enhanced Social Edge Services (SES) reliability than state-of-the-art approaches.

1. Introduction

The Social Internet of Things (SIoT) deployment increases daily, enabling social platforms to have a pervasive and immense impact on social media. IoT makes human life more modernized with 6G technology by forecasting the characteristics of intelligent sensors such as pervasiveness and heterogeneity. It is a herculean task to meet the application requirements and to maintain enamours generated data with specific computation resources. Mobile users often share information on social network platforms such as KakaoTalk, Twitter, Instagram, etc. It is therefore necessary to check the characteristics of the data owners to enhance data sharing privacy since most end-users are active on social platforms. In this regard, numerous researchers examined various methods to integrate trustworthiness communication history with fog computing scenarios to enhance social data and communication authenticity.

SIoT is defined as integrating social activities into IoT to share their information with encompassing gadgets [1]. SIoT has numerous benefits and challenges, like versatile organization establishment, proficient data trading, and stabling network orchestration. In this regard, Social Edge Service (SES) is an adaptive mechanism that deals with the above issues with the deployment of computing capacity servers and sensors that support low-dormancy data handling and delivery [2]. However, the availability of limited resources is a bottleneck for data computation and communication in edge-servers and high-density sensors [3]. Consequently, a limited coverage ratio influences the service completion time and data communication rate [4,5]. The SES also manages a broad scope of different fields, like online medical health, disaster detection [6], traffic and military surveillance [7].

Fog Computing (FC) enables sensing layer and network layer that supports SES to accomplish our objective [8]. FC prominently performs data fusion from multi-sources and brings down the computing service to the network-edge [9]. FC enables distributed computing features that help optimize network congestion, end-user security, and data privacy as per the arrived service request from users. However, FC characteristics

* Corresponding author.
E-mail addresses: msmekala@yu.ac.kr (M.S. Mekala), srivastavag@brandonu.ca (G. Srivastava), jessie@ynu.ac.kr (J.H. Park), hoyoul@yu.ac.kr (H.-Y. Jung).

https://doi.org/10.1016/j.dcan.2022.07.004
Received 29 May 2021; Received in revised form 9 June 2022; Accepted 8 July 2022
Available online 19 July 2022

suits to accomplish SES rather than traditional wireless sensor networks. In social data fusion, there are a few quandaries and trust assessment issues as follows:

1. Social data is vulnerable, which may cause system failure and computational overhead, and inadequate service reliability [10].
2. Social platforms may share false messages, which squander the transmission and computation assets.
3. Social data is large and has a complex structure that demands inadequate computation and communication resources, but the edge devices are not compatible due to limited storage and computation capacity.

Motivation: Social-user trust is assuredly a reliable measure to consolidate service reliability. Most of the investigations consider communication affecting factors or subjective strategies to measure trust-weight to make a trust decision system, which leads absence of versatility in trust aggregation computing. For instance, a service trust method has been designed based on transaction time, the total number of transactions and execution time attributes [11], but service trust is not categorized further effective communication between devices. In Ref. [12], the active trust function is designed based on the number of times the false data and real data are reported from the devices or vehicles through the probability distribution function. However, these state-of-art schemes have not considered complex SES network characteristics and key attributes during trust computing. Therefore, there is a need to design and develop an adaptive trust-weight measurement index and accurate channel selection model to enhance reliability and service quality.

SES aims to achieve adequate data sharing among the hooked devices such as sensors and servers to manage latency-constraint applications. Data-catching formulates the data re-transmission rate, which optimizes server overloaded issue [13]. The spectrum uses in 2-modes (Underlay and Overlay mode). The overlay mode permits sharing data through a pre-defined spectrum for enhancing throughput. In most cases, pre-defined resources use in underlay mode, but attention is essential for security attacks [14]. Considering the same spectrum to share the data causes attacks such as Jammer. Consequently, EDs privacy is more critical than spectrum efficiency. Therefore, establishing a secure communication channel is the main challenge to avoid computation and communication overhead of servers and active sensors in SIoT orchestration. The main constructions are as follows:

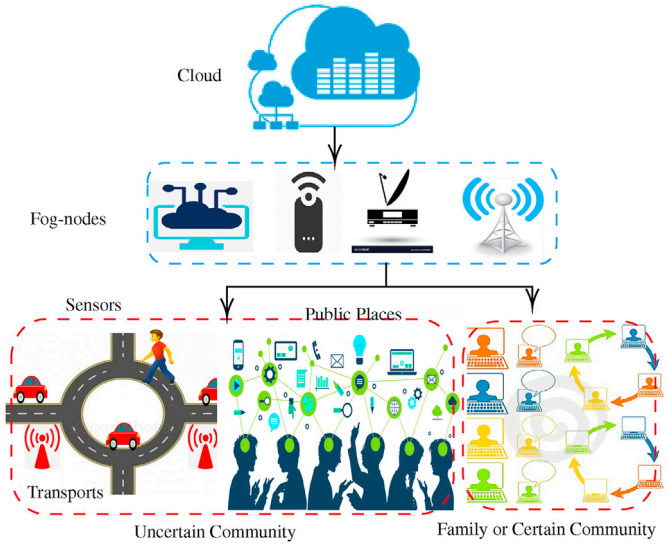


Fig. 1. Social-IoT orchestration.

1. Develop an Adaptive Trust Weight (ATW) model to estimate the fitness-priority of every node for consolidating the malicious node and reduce computation and communication overhead.
2. Develop a Quotient User-centric Coeval-Learning (QUCL) mechanism to formulate secure channel selection based on Nash equilibrium theory to reducing communication delay.
3. Simulations are carried out with social dataset and measurement indexes to examine the performance of our system.

Fig. 1 represents SIoT orchestration aspiration and importance. Generally, at the sensor level, the data or content is shared as per user request, but service classification and achieving high-ordered authenticity are challenging tasks to meet the deadline of delay-sensitive-social IoT applications. Subsequently, the monitoring region is divided into a social community or family community. Usually, the cross-validation is disproportionate for the family community since all family members are well known. The trust-weight value is consistently high compared to other communities. In addition, the uncertain community (social community) such as shopping malls, social places, gathered conference halls, public auditoriums are treated as numerous complex places because evaluating malicious devices is a Hercules task. In this regard, to classify such malicious devices, we design and develop an adaptive Hybridgraph Deep-learning Approach (HDA) with two innovative measurements called ATW and QUCL, which are described theoretically and mathematically in further sections.

The manuscript continues as Section 2 briefly explains research gaps and problem statements of extant approaches. Section 3 describes the proposed system and its mathematical models with novel algorithms in detail. Section 7 evaluates the investigation outcomes and Section 8 concludes the manuscripts.

2. Related work

In [15], home or office users are treated as friendly users; they confidently share data. Public auditoriums enable uncommon social-trust users, but still, they are considering a shared spectrum for data sharing, which is insecure [16]. Consequently, the authors used a socially-aware-model to distinguish trusted and untrusted clients depending on the social relationship strength. In Ref. [17], the security is measured based on the social relationships for complex networks and it considered binary values to decide whether the relation is trusty or not. However, the link quality and dynamic link status are not considered.

The primary use of social characteristics enhances the performance of intelligent applications by using the intrinsic relationship between content offloading and sharing. A socially-aware location privacy protection method is designed for vehicular networks [18,19]. A vehicular service access system is designed to enhance the service quality, and reliability of intelligent devices [20,21]. A trajectory data analysis model is designed for a traffic anomaly detection schemes for vehicle networks [22].

In [23], content caching policy is designed for secure social-aware communication based on social relations to diminish the download latency [24]. A conventional binary graph theory is considered to estimate robust device interference based on past examinations. Despite that, the complicated interference relationship is not yet designed by including node heterogeneity and densification, and a directed graph theory is used to estimate asymmetric inference relationships [25]. However, the security attributes are still not being considered during graph construction.

In [26], an efficient Personal Similarity Measurement (PSM) model is designed based on feedback from multi-resources to avoid attacks. However, the measurement model considers feedback from non-malicious devices, but the origin of the feedback is from malicious nodes. The mechanism mandates adaptive measures to classify non-malicious feedback and select secure channels to assess the sensor mode.

However, it is essential to design an HDA so as to address the above listed issues. In Ref. [27], a heuristic algorithm is designed based on a static-relay placement model called *Prophet* to enhance the performance

of social-sensor-links with the underlying objective of secure data sharing among the network. The mechanism is not revised for complex applications since the channel selection allocation approach does not integrate an eminent privacy mechanism for effective data sharing. In Ref. [28], a practical channel allocation approach is designed based on the hypergraph-colouring model for Device-to-device (D2D) communication. The sensor authentication system is considered before establishing the connection that causes communication and computation overhead.

Content Caching and User Association (JCC-UA) algorithms are used to mitigate the latency ratio of downloading content based on Smart Content Caching Policy (SCCP) and Dynamic User Association (DUA) [29,30]. An integrated node trust estimation method has been designed based on Bayesian inference considering penalty factors to enhance the privacy [31]. In Refs. [32–34], Energy Harvesting-Mobile Edge Computing (EH-MEC) approach has been designed to optimize the service offloading cost based on game theory and Lyapunov optimization theory. A User-centric resource-instance allocation has been designed based on virtual machine capacity to reduce the service execution delay for effective communication [35–37]. In this regard, an adaptive trust-weight measurement index and accurate channel selection model are designed to enhance social edge systems' reliability and service quality.

3. Proposed system model

Fig. 2 illustrates the system functioning mechanism, where the infrastructure enables 2-server nodes, 7-sensor nodes are interconnected through WiFi. Initially, the server system estimates each sensor's performance with related attributes to calculate the trust-weight of each sensor. Based on historical data, the threshold value or a benchmark is estimated to determine if a sensor is in the network for sensing and sending the data to the server or base station. The red communication indicates that the devices are in the trust assessment process. The blue communication indicates that the sensor is varified as a trusted node based on the average ATW value. If the ATW value remains abnormal, the sensor device is considered a Low-ATW Violation (LAV) sensor. Those sensors are maintained as an individual set for the observation to mitigate the generation of false data and communication, computation overhead.

In our proposed system, the sensors are classified into three types (High-ATW Violation (HAV) sensor, Low-ATW Violation (LAV) sensor, and Accurate-ATW sensor) based on the Adaptive Trust Weight (ATW) measurement, and the detailed description is covered in subsection 6.2. The LAV sensors might allow into the network as relay sensors because it may cause less overhead during computation-communication of data in the framework, i.e., $Q_{s_{i,k}}(I) \geq 0.5$. Besides, the HAV sensors cause a high overhead rate; such sensors are eliminated to avoid the generation of mysterious data as well as to reduce the overhead rate, i.e., $Q_{s_{i,k}}(I) \leq 0$. Accurate-ATW sensors ($Q_{s_{i,k}}(I) \leq 1$) are still active in the network for accomplishing the target. Table 1 consists of notation definitions.

3.1. Hybridgraph model

The hybridgraph constructs based on trust weight of social sensor and channel selection with asymmetric interference information. A hybridgraph $G = (S, L)$ enables a set of sensors $S = \{s_1, s_2, \ldots, s_i, \ldots, s_n\}$ with a set of links $L = \{l_1, \ldots, l_j, \ldots, l_m\}$. Every link has to meet two conditions, 1) $l_j \neq 0\ \forall l_j \in L$, and 2) $\underset{l_j \in L}{\cup} l_j = \frac{S(S-1)}{2}$, and each link l_j is hybrid-edge. The graph is formulated as $n \times m$ incidence matrix (U), i.e., $U = [u_{ij}]_{n \times m}$ and where $u_{ij} = 1$ *or* 0 means that, whether u_i belongs to l_j or not. Later, it is formulated as

$$u(i,j) = \begin{cases} 1, & s_i \in F(l_j) \\ -1, & s_i \in R(l_j) \\ 0, & \text{otherwise} \end{cases} \tag{1}$$

where $F(l_j)$ and $R(l_j)$ are front and rear of each edge. Let us assume, Δ_i denoted probability of adaptive trust weight (ATW) of sensor s_i to establish the secure connection between sensors (s_i,s_{i+1}) or sensor s_i to edge server (h_k) based on reliable channel quality. $l_j^{i,i+1}$ is j^{th} edge between sensors (s_i,s_{i+1}). Note that, $1 - \Delta_i = \hat{\Delta}_i$ is the probability of untrusted ATW value as per the link quality, and it is less than threshold value Θ_s of the sensor device. The sensor interfere (reciprocal behaviour) is used to formulate the graph as follows:

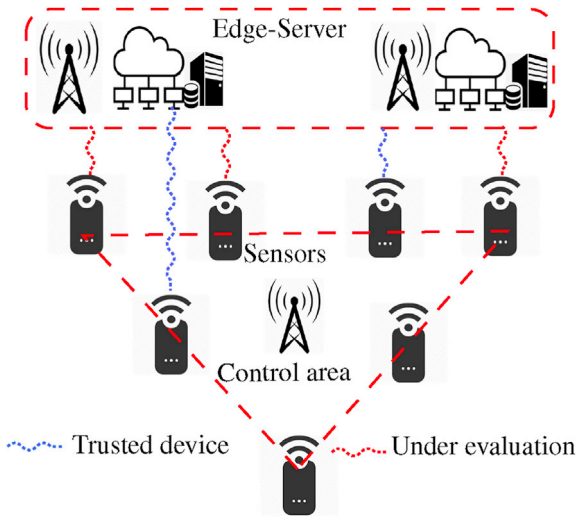


Fig. 2. System model.

$$\frac{\Delta_i \hbar_i s_i^t}{\sum\limits_{s_i \in s_n} \hat{\Delta}_{i,i+1} \hbar_{i+1} s_{i,i+1}^t} \leqslant \Theta_s \tag{2}$$

subsequently, edge server interference is used to formulate the graph based on threshold value Θ_k as follows:

$$\frac{\hbar_k s_{i,k}^t}{\sum\limits_{s_i \in s_n} (1 - \Delta_{i,k}) \hbar_i s_{i,i+1}^t} \leqslant \Theta_k \tag{3}$$

4. Problem formulation

The end-user inference is measured based on link quality of the edge l_j, and it is formulated as

$$v_{ij} = \begin{cases} 1, & if\ u(i,j) = -1 \\ 0, & if\ otherwise. \end{cases} \tag{4}$$

Definition 1. The connection between end-users (ED_q), $ED = \{ED_1$,

Table 1
Notation table.

Notation	Definition
κ_i^r, κ_k^r	Sensor probability of delivering r type service with s2s or s2server, respectively
$\lambda_i^r \lambda$	Sensor probability of executing the content on itself
Υ_k^r	Probability of server k to offload r type content to other server $k+1$
$\Im_k^r$	Amount of r type content offloading by k^{th} server
Γ_k^r	Residual capacity of k^{th} server
$\Re^r$	Required amount of computation (CPU cycles/sec)
Ψ_α^W	Data distribution policy with action set W
W^t	Action set $\lambda W^t = \{\lambda_i^r, \kappa_i^r, \Upsilon_k^r, \kappa_k^r, \Im_k^r, \varphi_{to}^r\}$
$\varkappa^t$	Policy gradient at time slot t
μ_i, μ_k	The multi-objective rank of sensor and server, respectively and should be in the range of [0,1]
$b_{p_k}^{s_k,t}$	Service execution quality rate of server at time t and it should be in range of [0,1]

ED_2, …, ED_q, …, ED_Q} forms an adaptive interference by choosing a secure channel $\wp$, which is formulated as

$$SR(\wp_q, \wp\hat{q}) = \sum_{l_j \in L} \eta_i(l_j) \times v_{ij} \text{Where } \eta_i = \begin{cases} 1, & \text{if } \wp_q \neq 0,\ \wp_q \in G \forall s_i \in l_j; \\ 0, & \text{if otherwise.} \end{cases} \tag{5}$$

where $\wp\hat{q}$ is the present channel of ED, which not yet select the channel and η_i is an indication factor. φ_i means the data sharing ability of sensor and '0' is the sensor which unable to share the data as follows:

$$\phi_i(\wp_q, \wp\hat{q}) = \begin{cases} 1, & \text{if } \wp_q \neq 0, SR(\wp_q, \widehat{\wp_q}) = 0; \\ 0, & \text{if otherwise.} \end{cases} \tag{6}$$

The problem is formulated as follows:

$$\max_{\wp_q \in \widehat{\wp_q}} \sum_{i=1}^{n} \phi_i(\wp_q, \wp\hat{q}),$$
$$Subject\ to: \phi_k(\wp_k, \wp\hat{k}) = 1 \ \ \forall \phi_k \in K \tag{7}$$

where $\varphi_k = 1$ means the secure communication between 2-edge-servers.

Definition 2. The data sharing requires asymmetric time because of various communication and computation strategies. The execution time of $r \in R$ service requests should meet their delay constraint $t_{\max}$, which is formulated as ƛ

$$\lambda_i^r \left(\kappa_i^r \varphi_t^r + \sum_{k=1}^{K} \kappa_k^r \hat{\varphi}_t^r - \sum_{k=1}^{K} \Upsilon_k^r \hat{\varphi}_t^r \right) + \sum_{k=1}^{K} \Upsilon_k^r \hat{\varphi}_t^r \tag{8}$$

Potential sensors receive their requested data to satisfy the time-sensitive constraints to diminish the communication overhead as follows:

$$\begin{aligned} &\underset{\lambda_i^r, \kappa_i^r, \Upsilon_k^r}{\text{Max}} \sum\nolimits_{r=1}^{R} \varphi_{to}^r \\ s.t\ \ &P_1 : \sum\nolimits_{r=1}^{R} \Re^r \left(\kappa_i^r \lambda_i^r + 1 \right) \times \Upsilon_k^r \\ &P_2 : \sum\nolimits_{k=1}^{K} \kappa_i^r \cdot \kappa_k^r = 1 \ \ \forall k \in K \end{aligned} \tag{9}$$

where P_1 denotes server computing capacity which should not be greater than its original computation capacity. P_2 means content distribution strategy between edge-sensors and sensor-to-server.

5. Effective computing and transmission models

Computation and transmission models play significant role in achieving effective performance of SIoT framework. Therefore, adaptive computing and transmission models are derived as follows to optimize the service reliability and performance.

5.1. Device-level computing

The device-level computing is also called as local computing. Let us assume, sensor s generates a set of computation intensive services $r_c^{s_i}{}_{s_i \in s_n} = \left(C_i, \Im_i^{r_c}, \mathrm{A}_i^{r_c}\right)$. Where C_i, $\Im_i^{r_c}$, $\mathrm{A}_i^{r_c}$ are total CPU cycles to execute the service, total data size for offloading, total data size of response revert to the requested sensor-node by the server respectively. The overhead of device-level computing is estimated as follows:

$$\aleph_{s_i}^{dl} = x_{s_i}^{\nabla} \nabla_{s_i}^{dl} + y_{s_i}^{\epsilon} \epsilon_{s_i}^{dl} \tag{10}$$

where $\nabla_{s_i}^{dl} = \frac{C_i}{\Re_{s_i}^{r_c}}$, $\epsilon_{s_i}^{dl} = C_i \times \epsilon_{c_i}^{s_i}$ time to execute the service request r, energy consumption respectively, and $\epsilon_{c_i}^{s_i}$ denotes energy usage per cycle. Subsequently, $y_{s_i}^{\epsilon}$, $x_{s_i}^{\nabla}$ denote weight of energy usage and weight of computation time, and $x_{s_i}^{\nabla} + y_{s_i}^{\epsilon} = 1$. The weight of computation time depends on computation service priority. Weighted payoff function is to fulfill the end-user requirements, and the basic strategy is: if the energy level is not prominent, then $y_{s_i}^{\epsilon}$ value will fix as greater to mitigate the energy usage. Similarly, during delay-sensitive service request execution, the $x_{s_i}^{\nabla}$ value will fix as greater to diminish delay ratio.

5.2. Edge-server level computing

Usually, when the sensor node is not capable $\leqslant \Re_{s_i}^{r_c}$ to execute the service, then a connection establishes between sensor and server based on ATW weight to execute the offloaded services on behalf of sensor node s_i, $i \varepsilon n$. In this scenario, the total service computation time is the sum of service offloading time through LTE interface for effective communication, service execution time by server, time required to revert the executed results to sensor node s_i, as follows:

$$\aleph_{s_i,k_i}^{sl} = x_{k_i}^{\nabla} \nabla_{s_i}^{sl} + y_{k_i}^{\epsilon} \epsilon_{k_i}^{sl} \tag{11}$$

where, the notation means server values

$$\nabla_{k_i}^{sl} = \frac{\left(\Im_i^{r_c} + \mathrm{A}_i^{r_c}\right)}{\beta_{s_i,k_i}^{t}} + \frac{C_i}{\Re_{k_i}^{r_c}} \ \beta_{s_i,k_i}^{t}$$
$$\epsilon_{k_i}^{sl} = \Im_i^{r_c} \times \epsilon_{c_i}^{s_i,k_i}$$

denotes data transmission rate which is formulated in the below subsection.

5.3. Transmission model

The data transmission rate of the service from sensor node to server through the selected channel $\wp_i$ is formulated based on shannon's theorem as

$$\beta_{s_i,k_i}^{t,\wp} = B_{\wp} \log_2 \left(1 + \frac{\rho_{s_i,k_i}^{t} \Lambda_{s_i,k_i}^{t}}{\zeta_{s_i,k_i} \cdot (d_{s_i,k_i})^2} \right) \tag{12}$$

where $B_{\wp}$, ζ_{s_i,k_i}, ρ_{s_i,k_i}^{t}, Λ_{s_i,k_i}^{t}, $(d_{s_i,k_i})^2$ denotes bandwidth of channel $\wp_i$, thermal noise power of channel, sensor node transmission power, channel gain of $\wp_i$ by sensor node due to path attenuation, distance between sensor node to server respectively. The transmission delay is related to the time required to offload the service and execution delay which is derived in the above section. The transmission time is expressed as

$$\phi_{s_i,k_i}^{t,\wp} = \frac{\Im_i^{r_c}}{\beta_{s_i,k_i}^{t,\wp}} \tag{13}$$

6. QUCL-secure channel selection

The channel selection graph construction is.

$G_{\wp} = \left(S, L, \{\hat{\wp}_i\}_{i=1}^{n}, \{X_i\}_{i=1}^{n}\right)$, where $\{\hat{\wp}_i\}_{i=1}^{n}$ is edge-devices available channel set, $\{X_i\}_{i=1}^{n}$ is utility and $\varphi_i(\wp_i, \wp_{i+1}) = \varrho_{i,i+1}$. Hence, Edge-device or sensor utility function is formulated as

$$X_i(\wp_i, \wp_{i+1}) = \varrho_{i,i+1} \times \left(1 + \sum\nolimits_{i,i+1\in n}^{N} \chi_{i,i+1}\right) \tag{14}$$

where $\wp_{i+1}$ is neighbor EU profile who has selected the secure channel. $\chi_{i,i+1}$ means whether s_{i+1} sensor has relation with s_i or not. The secure channel selection graph is consolidated with Eq. (15).

$$G_{\wp} = \max_{\wp_i \in \wp_i} X_i(\wp_i, \wp_{i+1}),\ \forall s_i \in S \tag{15}$$

Each EU-usage rate remaining is enhanced by consolidating the channel assessment process.

6.1. Secure data sharing

Secure data distribution is consolidated with HDL approach based on gradient mechanism with Eq. (9).

$$D\left(\lambda_i^r, \kappa_i^r, \Upsilon_k^r, \kappa_k^r\right) = \varphi_{to}^r - \sum\nolimits_{k=1}^{K} \Im_k^r \times \sum\nolimits_{r=1}^{R} \Re^r\left(\kappa_i^r \lambda_i^r + 1\right) \times \Upsilon_k^r - \sum\nolimits_{r=1}^{R} \sum\nolimits_{k=1}^{K} \Gamma_k^r \tag{16}$$

The gradient mechanism attentively measures the residual capacity of the server [38]; it will continue till the coverage of all sensors under the data request set.

$$\Gamma_k^r(l+1) = \left[\Gamma_k^r - l_k^r \left(\begin{array}{c} \varphi_{to}^r - \sum_{k=1}^{K} \Im_k^r \times \\ \sum_{r=1}^{R} \Re^r\left(\kappa_i^r \lambda_i^r + 1\right) \times \Upsilon_k^r - \sum_{r=1}^{R} \sum_{k=1}^{K} \Gamma_k^r \end{array}\right)\right]^+ \tag{17}$$

Two-Neural Network (NN) parameters α^z *and* α^{ϑ} are formulated for deep-learning process. Here, α^z is an actor function to consolidate the data distribution which is updated through primary neural network based on gradient policy and it is formulated as

$$\Psi_{\alpha}^{W} = F\left[\Psi_a \times \vartheta(l^t, W^t|\alpha^{\vartheta}) \Psi_{\alpha}^{W} z(W^t|\alpha^z)\right] \tag{18}$$

where, $\vartheta\left(l^t, W^t|\alpha^{\vartheta}\right) = F\left[z^t + \vartheta\left(W^{t+1}, z\left(W^{t+1}|\alpha^{\vartheta}\right)\right)\right]$ describes the action value and $z\left(l^{t+1}|\alpha^z\right)$ is a data distribution policy. α^{ϑ} is updated through primary criticism based on diminishing the error rate and it is defined as

$$Loss(\alpha^{\vartheta}) = F[Des^t - \vartheta(l^t, W^t|\alpha^{\vartheta})]^2 \tag{19}$$

$Des^t = s_i\left(l^t, W^t + \hat{\vartheta}\left(W^{t+1}, \hat{z}\left(W^{t+1}|\alpha\hat{z}\right)\right)\right)$ optimize the error impact during data coverage. Let us assume that, in the learning process, various trust weights are measured as per the area based on algorithm 3. In this regard, to diminish the loss rate, ensuring a linear convergence rate is essential, and in our simulation, the learning rate Φ is fixed.

Theorem 1. *Server selection policy and trust estimation policy are initialized with a minuscule deficiency margin mar concerning the destination Des equilibrium weights and depth of NN to meet the anticipated learning rate, as follows*

$$\Phi \leqslant \frac{mar^{(4\times depth-2)/depth}}{(depth)^3 \cdot \|Des_{n\times n}\|} \tag{20}$$

For any $error - ratio > 0$

The loss at every iteration (*iter*) is not significant as the error rate. In other words, the training loss drops to a low-error ratio with a linear convergence rate based on random initialization weights. The concerning simulation results are discussed in the below section.

$$iter \geqslant \frac{1}{\Phi \times mar^{2\cdot(depth-1)/depth}} \times \log\left(\frac{Loss(\alpha^{\vartheta})}{error - ratio}\right) \tag{21}$$

Algorithm 1: Reliable content sharing Approach when $0 \le Q_{s_{i,k}}(I) \le 0.5$

input : Sensor set $S[i]$, Edge-link set $L[j]$, $\lambda_i^r, \kappa_i^r, \Upsilon_k^r, \kappa_k^r$
output: Secure data distribution

1 Let $\lambda_i^r \neq 0$, $\kappa_i^r \neq 0$, $\Upsilon_k^r \neq 0$, $\kappa_k^r \neq 0$, $\forall \le 1$;
2 **for** *each* $s_i \in \boldsymbol{S}$ **do**
3 A feasible sensor set assessed based on Algorithm 3;
4 Estimate $D\left(\lambda_i^r, \kappa_i^r, \Upsilon_k^r, \kappa_k^r\right)$ using equation 16;
5 **while** $\Gamma_k^r \neq 0$ **do**
6 Estimate Eq.17;
7 $\Gamma_k^r(l+1) = \left[\Gamma_k^r - l_k^r \left(\varphi_{to}^r - \sum_{k=1}^{K} \Im_k^r \times \sum_{r=1}^{R} \Re^r\left(\kappa_i^r \lambda_i^r + 1\right) \times \Upsilon_k^r - \sum_{r=1}^{R} \sum_{k=1}^{K} \Gamma_k^r\right)\right]^+$;
8 **if** $\Gamma_k^r - (\Gamma_k^r(l+1)) \le \psi$ **then**
9 Requested service (content sharing) to be continued
10 **else**
11 Estimate the attributes of each social node to optimize the communication and computation overhead of edge-server (i.e, $\lambda_i^r, \kappa_i^r, \Upsilon_k^r, \kappa_k^r$)
12 **end**
13 **end**
14 **end**

Algorithm 1 measures the content sharing reliability to optimize the communication and computation overhead. The designed data sharing strategy adequately streamlines the objective based on the QUCL approach. The measurement attributes remain the same till the partial product outcome is less than the threshold (ψ). *Line* − 1 initializes the sensor and computation parameters. Line 2–3 assesses the concern parameters and list of sensors waiting to receive the content. Line 6–7 estimates each step-partial product for secure data sharing. Line 8 − 13 decides whether to continue the process or re-assess the listed attributes.

In Algorithm 2, the scheme $z(W^t|\alpha^z)$ formulates the secure data transmission over the requested region based on the UCL approach. The α^{ϑ} variable updates based on the error control loss function $Loss(\alpha^{\vartheta})$. Line-1 initializes the network parameters. Line-3 assesses the count of sensors which are requested to receive the content. Line 4–14 helps to accomplish the objective,i.e sharing the data securely over the requested network, after assessing the trust reliability factor of each sensor.

Reciprocal behaviour is considered to construct the trust communication graph between social users. Most existing systems have consider direct reciprocity, but our approach considers both direct, indirect edges, and it can be observed in Fig. 3. The reciprocal behaviour is derived based on the content sharing history. Basically, the edge means

Algorithm 2: QUCL approach for reliable content sharing to the demanded social range

input : Sensor set $S[i]$, Edge-link set $L[j]$, Data-sharing scheme $z(W^t|\alpha^z)$, neural network decision-factor $\vartheta\left(l^t, W^t|\alpha^\vartheta\right)$

output: Secure data distribution

1 Let initialize the factors α^z, α^ϑ;
2 **for** *each* $s_i \in \boldsymbol{S}$ **do**
3 Assess each iteration value; to make decision on attributes re-measurement;
4 **while** $\alpha^z \neq 0 \&\& \alpha^\vartheta \neq 0$ **do**
5 Estimate the
6 $\Psi_\alpha^W = F\left[\Psi_a \times \vartheta\left(l^t, W^t|\alpha^\vartheta\right)\Psi_\alpha^W z(W^t|\alpha^z)\right]$
7 based on Eq.18;
8 Update $\vartheta\left(l^t, W^t|\alpha^\vartheta\right) = F\left[z^t + \vartheta\left(W^{t+1}, z\left(W^{t+1}|\alpha^z\right)\right)\right]$;
9 Estimate
10 $Loss\left(\alpha^\vartheta\right) = F\left[Des^t - \vartheta\left(l^t, W^t|\alpha^\vartheta\right)\right]^2$ to optimize the loss rate based on Eq.19;
11 Update
12 $Des^t = s_i\left(l^t, W^t + \widehat{\vartheta}\left(W^{t+1}, \widehat{z}\left(W^{t+1}|\alpha^{\widehat{z}}\right)\right)\right)$;
13 **end**
14 Else go-to initial step and estimate attributes;
15 **end**

connection between $user_a$ and $user_b$ for data shared, which helps to construct the directed graph. The reciprocity behaviour is assessed based on a directed circle, and services between users are measured based on interaction time. Let us assume, algorithms 1 & 2 diverged into three sub-modules. First, the complexity of iterative measuring of server capacity is $O(n^2)$. Sorting the service requests based on social demand is an essential process and the complexity is $O(n\log_2 n)$. Third, content sharing request execution by the server is a significant process to satisfy the delay-sensitive social services, and the complexity is $O(n^3)$.

$$O(n^2) + O(n\log_2 n) + O(n^3) \tag{22}$$

6.2. Adaptive trust weight (ATW) measurement model

As a part of the secure communication process, node trust measurements are essential to reduce communication and computation overhead. In this regard, sensor-to-sensor communication is consolidated with network optimization parameters. Consequently, sensor service reliability rate is assessed based on service-feedback and sensor weight factor since brief information can be referred to in the previous work [39, 40]. The sensor correlation and sensor attributes are considered while estimating the ATW of s_k.

$$\xi(s_k, t) = \sum_{k=1}^{K} \mu_k b_{p_k}^{s_k,t} \tag{23}$$

After the selection of a channel, the sensor and server communicate as per service request and the communication quality is estimated as

$$\xi(s_{i,k}, t) = \sum_{i=1}^{n} \sum_{k=1}^{K} \mu_{i,k} b_{p_{i,k}}^{s_{i,k},t} \tag{24}$$

The server communication quality rate is considered, and the sensors communication quality is considered as well, but the measurement decisions are assessed based on threshold value. In this regard, the server communication quality for better performance of network is considered. Note:$i+1 = \hat{i}$

$$\xi(s_{i,\hat{i}}, t) = \sum_{i=1}^{n} \mu_{i,\hat{i}} b_{p_{i,\hat{i}}}^{s_{i,\hat{i}},t} \tag{25}$$

The communication quality weight is consolidated as follows

$$\varpi_{i,k} = \frac{1}{|S|} \times \left[\frac{\left|(\xi(s_k, t) - \xi(s_{i,k}, t)) + (\xi(s_k, t) - \xi(s_{i,i+1}, t))\right|}{\xi(s_k, t)}\right] \tag{26}$$

The ATW communication quality weight is classified to make accurate recommendation system and it is formulated as follows

$$Q_{s_{i,k}}(I) = \begin{cases} 0, & 0 \leqslant \varpi_{i,k} \leqslant \varpi_{i,k}^{thr_1} \\ 0.5, & \varpi_{i,k}^{thr_1} \leqslant \varpi_{i,k} \leqslant \varpi_{i,k}^{thr_2} \\ 1, & 0 \leqslant \varpi_{i,k} \leqslant 1 \end{cases} \tag{27}$$

$$0 \leqslant \varpi_{i,k}^{thr_1} \leqslant \varpi_{i,k}^{thr_2} \leqslant 1$$

While estimating the priority or recommendation of the potential server s_k, the server performance is considered. It is estimated by aggregating the weight factor $\nu_n = \frac{o_k}{(o_1+o_2+\cdots+o_n)}$. Here, ν_n is the total interaction between sensor s_i and server s_k. In case, $j = k$, $o_k = 0$, the ATW vector is formulated as $V_n(k) = (\nu_1, \nu_2, \ldots, \nu_n)$, the priority or recommendation of server is defined as follows:

$$\mathrm{Rec}_{i,k} = V_n(k) \times Q_{s_{i,k}}(I) \tag{28}$$

Algorithm 3 constructs the feasible sensor set and server set, determining which should be in the network to make a secure data distribution based on reliable trust analysis mechanism. Line 1–2 initializes the entailed variable. Line 4–5 estimates the individual sensor service quality as well as the servers. Line 6–7 assesses the infeasible sensors, which means those are unreliable. Line 8–13 helps make an accurate decision on which are suitable for secure communication and it impacts computation and communication overhead of the server.

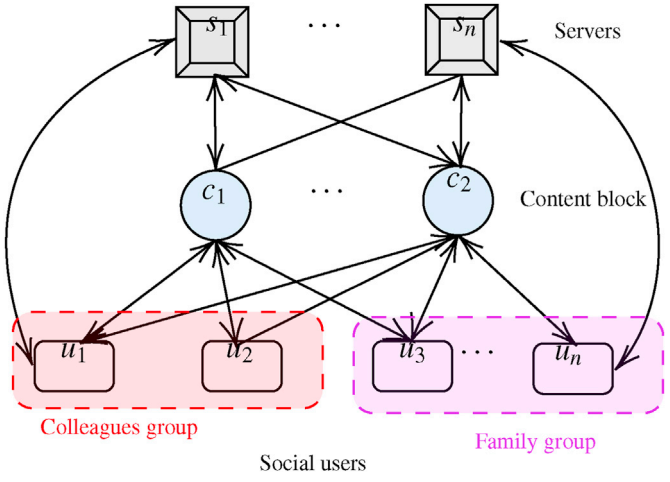


Fig. 3. Graph construction.

Algorithm 3: Reliable trust measurement

input : Sensor set S, Server set K, server initial weight μ_k, server initial service quality $b_{p_k}^{s_k,t}$
output: Recommendation or priority of sensor and server

Let $S = \{s_1, s_2, \cdots, s_i, \cdots, s_n\}$;
$\mu_k \neq 0, b_{p_k}^{s_k,t} \neq 0, \forall \leq 1$;
for *each* $s_i \in S$ **do**
  Estimate each sensor service quality at time t with Eq. 23, 24, 25;
  while $Q_{s_{i,k}} \neq 0$ **do**
    Estimate the reliable sensor trust matrix concerning to the time;
    if $0 \leq Q_{s_{i,k}} \leq 0.5$ **then**
      Update S[i] and k[i] set, recommended for local computing with deadline constraints;
    else
      Estimate u_n based on historical performance quality rate and feedback analysis;
      Estimate Re $c_{i,k} = V_n(k) \times Q_{s_{i,k}}(I)$ with Eq.28;
      Update feasible sets FS[i] and FSS[k];
    end
  end
end
Return reliable trust sensors

The complexity of measuring ATW score of each sensor node under heterogeneous environment is $O(n^2)$, since the number of cycles is n^2. The complexity of analysing the weight based on historical performance quality and feedback analysis is $O(n\log_2 n)$, but optimal complexity is $O(n^2)$ because of $O(n^2) \gg O(n\log_2 n)$.

Subsequently, the space complexity is derived as follows. Let assume: in our simulation k servers, each server can provide services for a set of s_i sensor nodes; as per the time window, the ATW measures are b number of times. In this process, the sensor node sends a trust-estimation request to the server and receives the response vice versa. The communication overhead of server is $2s_ib$, and s_ib is the overhead for direct communication between $s_i/s_{1+i}/k_i$ based on ATM information. The space complexity is derived as

$$
\begin{aligned}
&= k \times (s_i + 2s_i) \times b \\
&= (ks_i + k2s_i) \times b \\
&= ks_ib + k2s_ib \\
&= 3ks_ib
\end{aligned}
$$

7. Experimental results

The proposed HAD approach performance is measured with MATLAB 2017. The social network performance is analyzed with the NS3 simulator for partial cross-validation with node density and communication radius. The simulation parameters are listed in Table 2. Five hundred sensors are deployed in 500 × 500 area with a 50 m communication radius. Bandwidth is 200 KHz, maximum iterations are 400, video size varies from 1 to 100 Mb. The simulation is recursively conducted 95 times to observe the impact. The base parameters are considered [30] and the parameters are also adjusted as per paper objective demands based on decision-making graph theory [41]. INFOCOM from CRAWDAD datasets [42] are considered for performance examination.

Fig. 4(a) illustrated the variance in trust weight value between the untrusted node and trusted node. The node with a low-trust value is called an untrusted or non-recommended sensor node. The initial classification of low-trusted nodes impacts the computation and communication overhead of servers. Simulations are concurrently iterated more than 200 times to collect the data based on beta-distribution mean, which is fixed with 0.9. Each node is to be active 25 times during data collection. During initial iterations, the trust-value is normal, and 35–50 iterations also the trust-value remains constant; but from 20 to 35, the trust-value is abnormal. In Fig. 4(b), the impact of low-trusted-value nodes on communication is described. The active node's trust value constantly quits with a considerable communication ratio. In each iteration, the sensors'abnormal rate and the possibilities of receiving the shared data have been examined. From iterations 15–25, the low-trust nodes are not permitted to collect the data in the network, which creates communication overhead. After iteration 35, the active sensor nodes ratio increases and remains constant for network sustainability. The outcome plays a vital role in assessing the mode-decision of a sensor to enhance the effectiveness of our approach.

The data transmission rate of social-IoT framework has been examined with network throughput parameter and the completion time of service is more accurate than state-of-art approaches (PSM, hypergraph-colouring model, Prophet models), and the results are represented in Fig. 5(a). The low-trust sensors performance is assessed based on total packets collected by the base station and the rate of successful data transmissions towards the base station. Note that the x-axis is the percentage of total deployed sensors over the network. The HAD approach has achieved less-data collection rate from Low-ATW-V (LAV) sensor nodes, and few LAV sensors have a provision for sharing the data with non-LAV sensor nodes; but in PSM, most LAV sensors are allowed to share and send data to the servers, which influences the communication and computation overhead of the servers. The offloading-decision rate of LAV sensors is comprehensively examined and analyzed; the results are represented with Fig. 5(b). The offloading decision rate is collectively decreased as the LAV sensor percentage increases. Optimization of false data generation source mechanism essentially has an influence on reducing server computation overhead. The PSM, hypergraph-colouring, and Prophet models achieved high data-offloading rate than our approach because the secure channel selection method and ATW model have assessed the sensor state before the concerned node sends the data to the server or another sensor.

Fig. 6(a) illustrates the comparative analysis between active sensors and their impacts on the average communication rate. Our approach has achieved an effective communication rate because algorithms 1 and 2 consolidate the data-sharing issue with the UCL model through a deep-learning mechanism. The PSM approach shares the data without consideration of sensor-sensor delivery rate and available resources rate. In our approach, a vast number of sensors share the data concerning delay-sensitive service requests because of an effective learning mechanism, which is defined under the RUCL approach Section 7. Online data delivery through sensor-to-sensor communication mode is an efficient strategy for data dispatch, which is a solid addition to the computation offloading and sensor-server distribution methods.

Fig. 6(b) shows a sensor-based quotient correlation model to construct a hybrid-graph with directed edges to assess their status through a deep learning mechanism that comes under the quotient-UCL model. During each iteration, the sensor is allowed when it has a correlation with neighbor sensors or with consequent sensors. The rest of the active sensors are not allowed in the same communication channel during the data sharing. The sensor count is adjusted and equated to the iteration count based on the state-of-art approaches to examine the error rate. It is noted that the sensor count increases as the increment of iteration account; if the edge count increases, the communication rate decreases since edge number and communication ratio are inversely

Table 2
Simulation parameters.

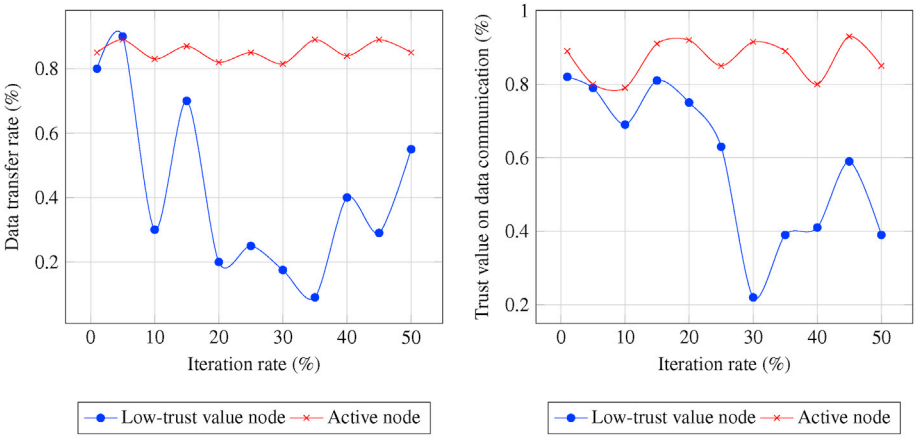
Parameter	Values
Area size (m^2)	500 × 500
Number of sensors	1000
Sensor radius	50 m
Number of edge-servers	50
Server radius	500 m
Window size	100 s
Trust measurement range	0–1
Θ_s and Θ_k	25 dBm, 15 dBm
Bandwidth	200 KHz
Max-Iterations	400
Video size	0–100 Mbits

dependent on each other. The increased iteration count denotes the communication rate optimality to share the data as per the sensor demand.

Fig. 7 illustrates the comparative analysis of the node computation capacity rate and their offloading decision rate concerned with social-IoT framework size. During simulation, two different cases to assess the performance are considered. First, *$s = 500$, $K = 5$, and node-density $= 0.05$* to estimate sensor computation capacity, which is an essential factor to in achieving high network reliability. While increasing the computation capacity rate of the sensor, the offloading decision is being drastically reduced. It is noted that the active sensor count plays an important role in offloading decisions. Here, the considered active sensor set has a normal ATW value that can be observed in Fig. 7(a). In the second case, while increasing the server count 5-to-15, and the node density level is 0.05-to-0.15. Almost $\frac{1}{3}$ has the increased resource capacity of the network, which influences the offloading decision rate, and it is often lower than the previous case in Fig. 7(b).

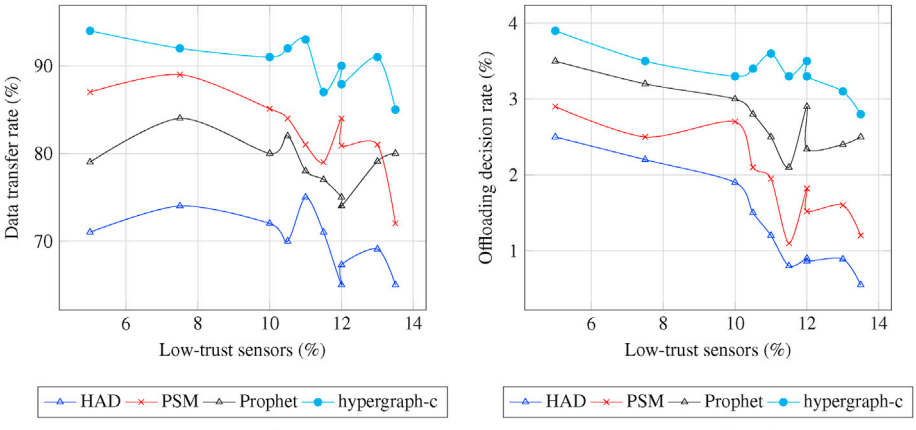
Fig. 8 illustrates the secure channel selection strategies which impact the execution of demanded service requests. When server count is equal to 3, the server computation rate is measured between 1% and 5%, but the increase of server count from 3–12 influences computation and communication overhead rate to accomplish our manuscript objective. Therefore, the classification of LAV sensors and secure channel selection schemes measure the notable impacts on social edge service with expected reliability.

In the learning simulation process, the hyperparameters are initialized as follows: the learning rate is 0.001, the batch size is 125, the number of epochs is 60, and usual parameters like 32 inputs, 32 steps, 10-outputs and the number of batches are 100 for each simulation scenario. Fig. 9 illustrates the analysis of learning impact based on the error rate for each epoch. The error rate is achieved less than 0.009 at the average learning rate of $\Phi \leqslant 0.007$ with less than 20 epochs. Hence, an average error ratio with low loss and an adequate learning rate are achieved. In the first scenario, the simulation results are measured, and the error rate is $\leqslant 0.2$ with a maximum learning rate $\Phi \leqslant 0.015$ and 60 maximum epochs. An accurate policy learning rate ($\Phi \leqslant 0.05$) is achieved for subsequent learning trials and adequate convergence steps based on subsequent weight adjustments to mitigate the loss ratio.



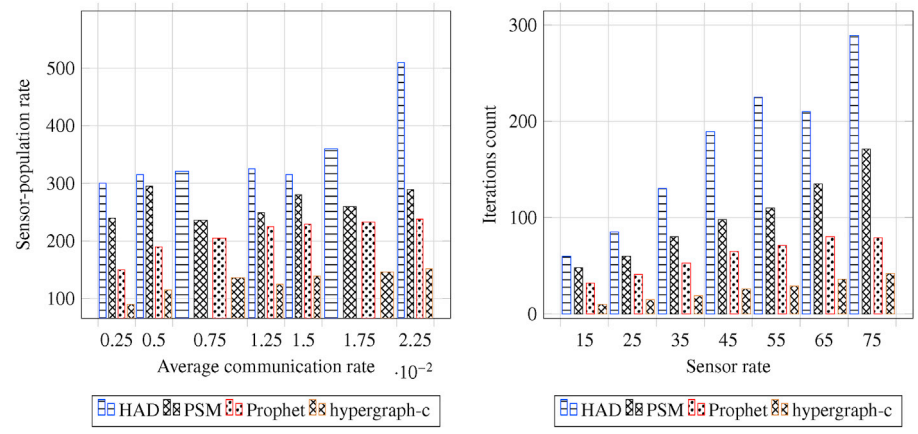
(a) Trust value vs data collection (b) Trust value vs data communication

Fig. 4. Iterations and trust-weight rate analysis.



(a) Low-trust sensor rate vs data transfer rate (b) Trust value vs offloading decision rate

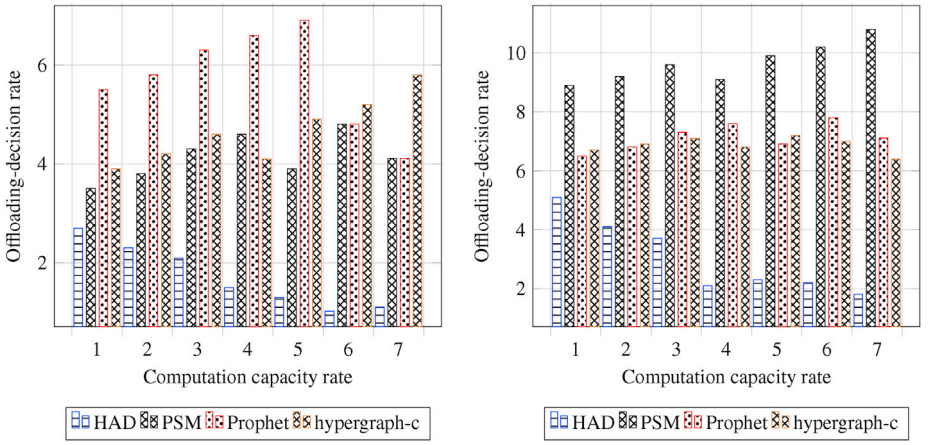
Fig. 5. Impact of LAV sensors on data transmission and offloading rate.



(a) Average communication rate vs Received data sensors

(b) sensor-rate vs iterations count

Fig. 6. Average communication rate and iteration rate analysis.



(a) $S = 600, K = 15, Node - density = 0.15$

(b) $S = 500, K = 5, Node - density = 0.05$

Fig. 7. Offloading decision rate and computation rate analysis when a)$S = 600$, $K = 15$, $Node - density = 0.15$ and b) $S = 500$, $K = 5$, $Node - density = 0.05$.

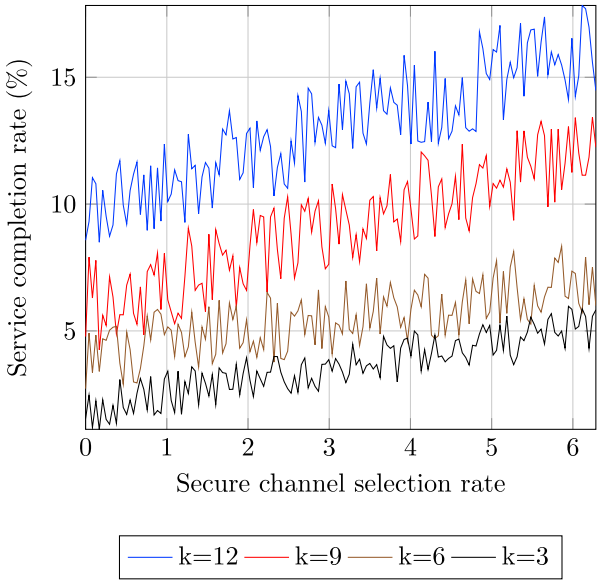


Fig. 8. Channel selection impact analysis on social data-sharing.

Fig. 10 illustrates convergence steps to adjust the behaviour of weights to meet the targeted accuracy of our approach with the adaptive initial fixed learning rate, i.e., $\Phi = 0.0039$. However, the convergence steps vary as per the trials and learning rate to achieve adequate accuracy. When convergence steps (approximately 295) are moderately high,

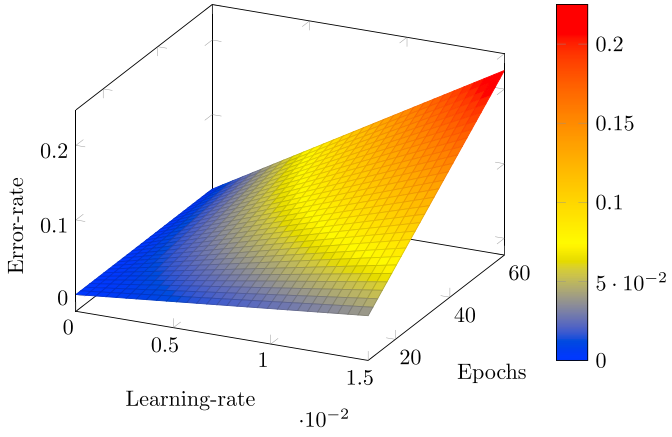


Fig. 9. Learning rate impact analysis on error rate concerning epochs.

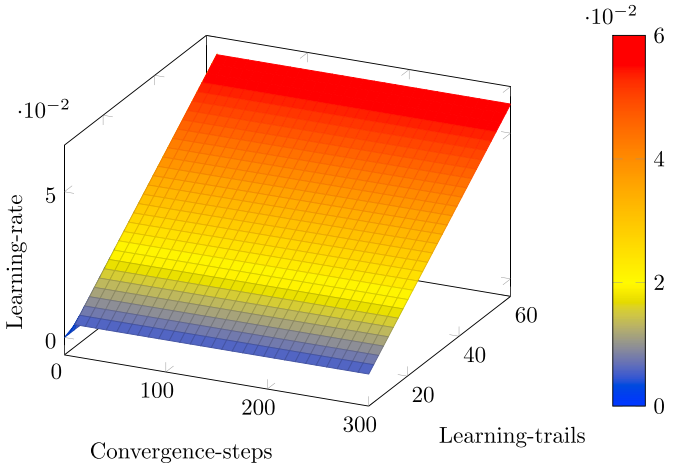


Fig. 10. Impact of learning rate and convergence ratio.

the policy learning rate is at $\Phi = 0.0039$; but it comes to an increase of learning trails with adequate convergence steps (average 155), the policy learning rate has increased drastically; such as convergence rate increased as increasing the learning rate from $\Phi = 0.0039$ to $\Phi = 0.06$.

8. Conclusion

This paper presents HAD approach based on a two-step reliable trust communication and computation model for securing social-IoT networks. The designed HAD approach achieves an average 31% performance better than state-of-art approaches. HAD approach achieves a higher privacy preservation rate to protect from active or passive attacks based on a novel trust measurement index. Trust priority is estimated for every intelligent device (roadside units, mobile edge devices, server) to optimize computation and content sharing overhead. The designed Adaptive Trust Weight (ATW) model effectively assesses the node fitness priority to identify the malicious nodes based on a relation-based feedback fusion analysis report. The User-centric Coeval-Learning (UCL) mechanism essentially considers the trust weight value to select a channel for achieving secure communication, and the Nash equilibrium theory helps mitigate the communication delay while sharing data over edge devices.

Declaration of competing interest

The authors declare the following financial interests/personal relationships which may be considered as potential competing interests:

Acknowledgments

This work is supported in part by Basic Science Research Programs of the Ministry of Education (NRF-2018R1A2B6005105) and in part by the National Research Foundation of Korea (NRF) grant funded by the Korean government (MSIT) (No.2019R1A5A8080290).

Appendix

Theorem: The channel selection mechanism enables Nash equilibrium to enhance the system accuracy based on algorithms 1 and 2 with potential function $\partial(\wp_q, \wp\hat{q})$ and it satisfies. $X_q(\wp_q, \wp\hat{q}) - X_q(\wp_q, \wp\hat{q}) = \partial(\wp_q, \wp\hat{q}) - \partial(\wp_q, \wp\hat{q})$

Proof: To goal can accomplished by optimizing problem 9. The fixed potential function is $\partial(\wp_q, \wp\hat{q}) = \sum_{i,i+1\in n}^{N} \varphi_i(\wp_q, \wp\hat{q})$. In each iteration, the EU or ED may change their selected channel from $\wp_q$ to $\wp_q$, then the potential function is formulated as

$$\partial(\wp_q, \wp\hat{q}) - \partial(\overline{\wp_q}, \wp\hat{q}) = [\phi_q(\wp_q, \wp\hat{q}) - \phi_i(\overline{\wp_q}, \wp\hat{q})] + \left[\sum_{q+1\in Q} (\phi_{q+1}(\wp_{q+1}, \wp_{\widehat{q+1}}) - \phi_i(\overline{\wp_{q+1}}, \wp_{\widehat{q+1}}))\right] + \sigma(Q/(q \cup q+1)) \tag{29}$$

where $\sigma(Q/(q \cup q+1))$ is the variance ratio of potential function based on $\wp_q$ and $\wp_q$. Eq. (15) is formulated as follows.

$$\sum_{q+1\in Q} (\varphi_{q+1}(\wp_{q+1}, \wp_{\widehat{q+1}}) - \varphi_i(\overline{\wp_{q+1}}, \wp_{\widehat{q+1}})) = \left[\sum_{q+1\in Q} (\varphi_{q+1}(\wp_{q+1}, \wp_{\widehat{q+1}}))\chi_{i,i+1} - \sum_{q+1\in Q} (\varphi_{q+1}(\overline{\wp_{q+1}}, \wp_{\widehat{q+1}}))\chi_{i,i+1}\right]$$
$$+\left[\sum_{q+1\in Q} (\phi_{q+1}(\wp_{q+1}, \wp_{\widehat{q+1}}))(1-\chi_{i,i+1}) - \sum_{q+1\in Q} (\phi_{q+1}(\overline{\wp_{q+1}}, \wp_{\widehat{q+1}}))(1-\chi_{i,i+1})\right] \tag{30}$$

For Eq. (6), the final iteration value is equal to *zero*, since $\chi_{i,i+1} = 1$, i.e., EU q_{i+1} is correlated with q_i. In case, $\chi_{i,i+1} = 0$, i.e., EU q_{i+1} is not correlated with q_i, then the $\phi_{q+1}(\wp_{q+1}, \wp_{\widehat{q+1}}) - \phi_i(\overline{\wp_{q+1}}, \wp_{\widehat{q+1}})$ is equal to zero, which confines that the final iteration value is equal to *zero*. Therefore, LHS = RHS.

References

[1] L. Atzori, A. Iera, G. Morabito, M. Nitti, The social internet of things (siot)–when social networks meet the internet of things: concept, architecture and network characterization, Comput. Network. 56 (16) (2012) 3594–3608.
[2] M. Liu, F.R. Yu, Y. Teng, V.C. Leung, M. Song, Computation offloading and content caching in wireless blockchain networks with mobile edge computing, IEEE Trans. Veh. Technol. 67 (11) (2018) 11008–11021.
[3] N. Zhao, F. Cheng, F.R. Yu, J. Tang, Y. Chen, G. Gui, H. Sari, Caching uav assisted secure transmission in hyper-dense networks based on interference alignment, IEEE Trans. Commun. 66 (5) (2018) 2281–2294.
[4] T.-D. Nguyen, E.-N. Huh, M. Jo, Decentralized and revised content-centric networking-based service deployment and discovery platform in mobile edge computing for iot devices, IEEE Internet Things J. 6 (3) (2018) 4162–4175.
[5] M. S, P. Rizwan, M.S. Khan, Computational intelligent sensor-rank consolidation approach for industrial internet of things (iiot), IEEE Internet Things J. 10 (3) (2023) 1, https://doi.org/10.1109/JIOT.2021.3073600.
[6] S. Rani, S.H. Ahmed, R. Talwar, J. Malhotra, Can sensors collect big data? an energy-efficient big data gathering algorithm for a wsn, IEEE Trans. Ind. Inf. 13 (4) (2017) 1961–1968.
[7] K. Nakashima, M. Yokoyama, Y. Taniyama, T. Yohshihisa, T. Hara, s3 system: a system for sharing social sensor data and analytical programs, in: Adjunct Proceedings of the 13th International Conference on Mobile and Ubiquitous Systems: Computing Networking and Services, 2016, pp. 147–152.
[8] P. Singh, Y.K. Dwivedi, K.S. Kahlon, R.S. Sawhney, A.A. Alalwan, N.P. Rana, Smart monitoring and controlling of government policies using social media and cloud computing, Inf. Syst. Front 22 (2) (2020) 315–337.
[9] A. Chakraborty, S. Misra, A. Mondal, QoS-Aware Dynamic Cost Management Scheme for Sensors-as-a-Service, *IEEE Transactions on Services Computing* 15 (3) (2022) 1720–1731, https://doi.org/10.1109/TSC.2020.3011495.

[10] J. Liang, M. Zhang, V.C. Leung, A reliable trust computing mechanism based on multisource feedback and fog computing in social sensor cloud, IEEE Internet Things J. 7 (6) (2020) 5481–5490.
[11] M.J. Aslam, S. Din, Defining service-oriented trust assessment for social internet of things, IEEE Access 8 (2020) 206459–206473.
[12] J. Guo, Wang, A lightweight verifiable trust based data collection approach for sensor–cloud systems, J. Syst. Architect. 119 (2021), 102219.
[13] M. Ji, G. Caire, A.F. Molisch, Fundamental limits of caching in wireless d2d networks, IEEE Trans. Inf. Theor. 62 (2) (2015) 849–869.
[14] S. Ghosh, T. Acharya, S.P. Maity, On outage analysis in swipt enabled bidirectional d2d communications using spectrum sharing in cellular networks, IEEE Trans. Veh. Technol. 69 (9) (2020) 10167–10176.
[15] X. Chen, Y. Zhao, Y. Li, X. Chen, N. Ge, S. Chen, Social trust aided d2d communications: performance bound and implementation mechanism, IEEE J. Sel. Area. Commun. 36 (7) (2018) 1593–1608.
[16] M. Ahmed, Y. Li, Z. Yinxiao, M. Sheraz, D. Xu, D. Jin, Secrecy ensured socially aware resource allocation in device-to-device communications underlaying hetnet, IEEE Trans. Veh. Technol. 68 (5) (2019) 4933–4948.
[17] K. Zheng, J. Zhang, X. Liu, L. Fu, X. Wang, X. Jiang, W. Zhang, Secrecy capacity scaling of large-scale networks with social relationships, IEEE Trans. Veh. Technol. 66 (3) (2016) 2688–2702.
[18] B. Ying, A. Nayak, A distributed social-aware location protection method in untrusted vehicular social networks, IEEE Trans. Veh. Technol. 68 (6) (2019) 6114–6124.
[19] A.M. Vegni, C. Souza, V. Loscri, E. Hernandez-Orallo, P. Manzoni, Data transmissions using hub nodes in vehicular social networks, IEEE Trans. Mobile Comput. 19 (7) (2019) 1570–1585.
[20] Z. Ning, X. Hu, Z. Chen, M. Zhou, B. Hu, J. Cheng, M.S. Obaidat, A cooperative quality-aware service access system for social internet of vehicles, IEEE Internet Things J. 5 (4) (2017) 2506–2517.
[21] G. Epiphaniou, P. Karadimas, Ismail, Nonreciprocity compensation combined with turbo codes for secret key generation in vehicular ad hoc social iot networks, IEEE Internet Things J. 5 (4) (2017) 2496–2505.
[22] Z. Ning, Vehicular social networks: enabling smart mobility, IEEE Commun. Mag. 55 (5) (2017) 16–55.
[23] J. Li, Liu, On social-aware content caching for d2d-enabled cellular networks with matching theory, IEEE Internet Things J. 6 (1) (2017) 297–310.
[24] H.-R. Cheon, J.-H. Kim, Social-aware mobile data offloading algorithm through small cell backhaul network: direct and indirect user influence perspectives, Comput. Network. 165 (2019), 106951.
[25] Y. Sun, Du, Directed-hypergraph-based channel allocation for ultradense cloud d2d communications with asymmetric interference, IEEE Trans. Veh. Technol. 67 (8) (2018) 7712–7718.
[26] J. Yuan, X. Li, A reliable and lightweight trust computing mechanism for iot edge devices based on multi-source feedback information fusion, IEEE Access 6 (2018) 23626–23638.
[27] X. Zhang, G. Cao, Proactively placing static relays with social-link awareness in mobile social networks, IEEE Trans. Veh. Technol. 68 (2) (2018) 1903–1915.
[28] H. Zhang, L. Song, Z. Han, Radio resource allocation for device-to-device underlay communication using hypergraph theory, IEEE Trans. Wireless Commun. 15 (7) (2016) 4852–4861.
[29] Y. Li, H. Ma, L. Wang, S. Mao, G. Wang, Optimized content caching and user association for edge computing in densely deployed heterogeneous networks, IEEE Trans. Mobile Comput. 21 (2020) 2130–2142.
[30] M.S. Mekala, A. Jolfaei, G. Srivastava, X. Zheng, A. Anvari-Moghaddam, P. Viswanathan, Resource offload consolidation based on deep-reinforcement learning approach in cyber-physical systems, IEEE Trans. Emerging Topics Comput. Intell. 6 (2) (2022) 245–254, https://doi.org/10.1109/TETCI.2020.3044082.
[31] H. Gao, C. Liu, Y. Yin, Y. Xu, Y. Li, Hybrid Approach to Trust Node Assessment and Management for VANETs Cooperative Data Communication: Historical Interaction Perspective, in, *IEEE Transactions on Intelligent Transportation Systems* 23 (9) (2022) 16504–16513, https://doi.org/10.1109/TITS.2021.3129458.
[32] S. Xia, Z. Yao, Y. Li, S. Mao, Online distributed offloading and computing resource management with energy harvesting for heterogeneous mec-enabled iot, IEEE Trans. Wireless Commun. 20 (10) (2021) 6743–6757.
[33] Y. Li, C. Liao, Y. Wang, C. Wang, Energy-efficient optimal relay selection in cooperative cellular networks based on double auction, IEEE Trans. Wireless Commun. 14 (8) (2015) 4093–4104.
[34] H. Gao, Y. Zhang, H. Miao, et al., SDTIOA: Modeling the Timed Privacy Requirements of IoT Service Composition: A User Interaction Perspective for Automatic Transformation from BPEL to Timed Automata. *Mobile Netw Appl* 26 (2021) 2272–2297, https://doi.org/10.1007/s11036-021-01846-x.
[35] Y. Huang, H. Xu, H. Gao, X. Ma, W. Hussain, Ssur: an approach to optimizing virtual machine allocation strategy based on user requirements for cloud data center, IEEE Trans. Green Commun. Networking 5 (2) (2021) 670–681.
[36] X. Ma, H. Xu, H. Gao, M. Bian, Real-time multiple-workflow scheduling in cloud environments, IEEE Trans. Network Serv. Manag. 18 (4) (2021) 4002–4018.
[37] M.S. Mekala, W. Park, G. Dhiman, et al., Deep Learning Inspired Object Consolidation Approaches Using LiDAR Data for Autonomous Driving: *Arch. Comput. Methods Eng.* 29 (2022) 2579–2599, https://doi.org/10.1007/s11831-021-09670-y.
[38] M.S. Gaurav, G. Srivastava, Z. Nain, H. Zhang, W. Viriyasitavat, G.P.S. Varma, A drl-based service offloading approach using dag for edge computational orchestration, IEEE Trans. Comput. Social Syst. (2022) 1–9, https://doi.org/10.1109/TCSS.2022.3161627.
[39] M. Mekala, P. Viswanathan, Equilibrium transmission bi-level energy efficient node selection approach for internet of things, Wireless Pers. Commun. 108 (3) (2019) 1635–1663.
[40] G. Dhiman, Patan, Deep learning-influenced joint vehicle-to-infrastructure and vehicle-to-vehicle communication approach for internet of vehicles, Expet Syst. 39 (5) (2021), e12815.
[41] J. Wallenius, J.S. Dyer, P.C. Fishburn, R.E. Steuer, S. Zionts, K. Deb, Multiple criteria decision making, multiattribute utility theory: recent accomplishments and what lies ahead, Manag. Sci. 54 (7) (2008) 1336–1349.
[42] B. Köksal, R. Schmidt, X. Vasilakos, N. Nikaien, Crawdad dataset, URL, https://crawdad.org/umkc/networkslicing5g, 2019.