

© 2023 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

Rehman, Amjad, Khalid Haseeb, Teg Alam, Faten S. Alamri, Tanzila Saba, and Houbing Song. "Intelligent Secured Traffic Optimization Model for Urban Sensing Applications with Software Defined Network." IEEE Sensors Journal, 2023, 1–1. <https://doi.org/10.1109/JSEN.2023.3331311>.

<https://doi.org/10.1109/JSEN.2023.3331311>

Access to this work was provided by the University of Maryland, Baltimore County (UMBC) ScholarWorks@UMBC digital repository on the Maryland Shared Open Access (MD-SOAR) platform.

Please provide feedback

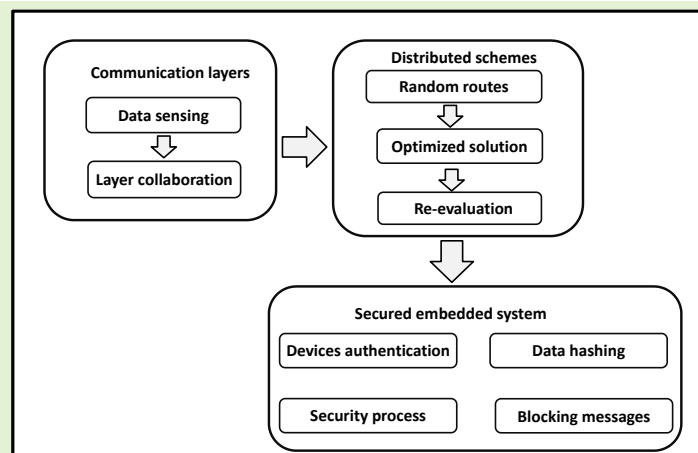
Please support the ScholarWorks@UMBC repository by emailing scholarworks-group@umbc.edu and telling us what having access to this work means to you and why it's important to you. Thank you.

Intelligent secured traffic optimization model for urban sensing applications with Software Defined Network

Amjad Rehman¹, Khalid Haseeb¹, Teg Alam², Faten S. Alamri^{3,*}, Tanzila Saba¹, Houbing Song⁴

Abstract— Smart communication using sensors and wireless structures is gaining rapid growth from remote sensing across the globe. Many surveillance systems use next-generation Internet of Things (IoT) technologies to get online data over the distributed network. Such a system speeds up daily routing communication and increases data observation efficiency for urban areas. In recent decades, many solutions have been developed to overcome data fusion problems in urban sensing systems. However, numerous approaches are still needed to build learning algorithms for heterogeneous networks with adequate transmission delays. Such networks are required to manage wireless technologies effectively while transporting massive data toward a cloud network. Furthermore, unauthorized devices with controlling computing capabilities should be kept away from network services. This work presents a protocol for Distributed Fault Tolerant Data sharing (DFTDS) in smart cities with security by exploring Software Defined Network (SDN) technologies and offers the most reliable urban network. Firstly, heterogeneous nodes and devices establish collaborative strategies for collecting and distributing the data on the low-constraint links with intelligent collaborative methods. Secondly, using the self-organizing scheme, the nodes are distributed over the paths and achieve green communication with global optimization criteria. In the end, the hashing scheme increases security levels for devices in terms of privacy and verification against network anomalies. The performance results show effective outcomes for packet delivery, network latency, link disconnection, network complexity, and alive nodes in dynamic scenarios as compared to other work.

Index Terms— optimization criteria; urban cities; security; public infrastructure; blockchain



I. Introduction

Sensors and Internet technologies resolve numerous urban problems to facilitate heterogeneous network and data applications [1, 2]. This network transports a large amount of multi-type data from the observing environment and simplifies the data analysis process in smart cities [3-5]. Real-time heterogeneous data is processed on the network edges and further forwarded toward centralized storage with the support of urban sensors [6-8]. However, on the other hand, IoT systems generate numerous events and incur overloads on the edges. Unbalanced and heterogeneous network traffic causes excessive latency, information loss, and a lower packet delivery ratio in many emerging applications [9-11]. Smart items and their implementations need to grow for automatic data collection and analysis-based decisions. As a result of the wide

range of IoT data, researchers are trying to develop intelligent solutions based on machine learning to reduce the complexity of urban sustainability with the consideration of security and network congestion [12-14].

Moreover, before sending data to the central station, edges should remove redundancies from surrounding nodes' data [15, 16]. However, most solutions cannot balance the traffic flowing among the devices while carrying a high amount of data over distributed networks. In addition, due to the heavy load, many links fail during the routing step, resulting in higher retransmission costs [17-19]. Moreover, security is another primary goal for emerging networks to keep the privacy and authenticity of collected information [20-22]. Adopting a secured communication system gives the surety for data availability for the embedded networks. IoT networks are

¹Artificial Intelligence & Data Analytics (AIDA) Lab CCIS, Prince Sultan University, Riyadh 12435, Saudi Arabia; email: arkhan@psu.edu.sa, khaseeb@psu.edu.sa, tsaba@psu.edu.sa

²Department of Industrial Engineering, College of Engineering, Prince Sattam bin Abdulaziz University, Al Kharj-11942, Kingdom of Saudi Arabia, email: t.alam@psau.edu.sa

³Department of Mathematical Sciences, College of Science, Princess Nourah Bint Abdulrahman University, P.O.Box 84428, Riyadh, 11671, Saudi Arabia. email: fsalamri@pnu.edu.sa

⁴Department of Information Systems, University of Maryland, Baltimore County (UMBC), Baltimore, MD 21250 USA; email: h.song@ieee.org

performing a key role in collecting data and forwarding it toward edges with wireless systems. Although numerous solutions have been proposed for urban cities to balance traffic load among IoT channels and improve end-user performance. However, it was noticed that a variety of applications are based on mobile devices, in such cases, routing costs are very high due to breakages and the number of request packets. In addition, protecting the route from unidentified devices is a significant research challenge. Thus, this work proposes a model using SDN architecture to reduce the additional overheads on the IoT infrastructure and monitor the environment through frequent analysis. Also, using security codes, the faulty nodes are identified intelligently for data receiving and forwarding toward requested nodes. This research study explores a greedy local optimization strategy for handing over heterogeneous IoT data using SDN architecture to allow distributed data-sharing and lessen the network load.

SDN controller removes such links from the forwarding tables and effectively manages the network distribution to ease the congested communication caused by excessive traffic flow on the IoT network. Moreover, peer connections are more trustworthy because of blockchain-based data privacy and authentication. In terms of reliable processing for data from multiple types of nodes and a reduction in computing costs, the DFTDS facilitates smart cities.

The following are the key contributions of the proposed work.

- i. The over-computing communication links are identified and accordingly forwarding methods are dynamically managed with adaptive solutions. This technique decreases transmission time while sending heterogeneous data in urban sensing applications.
- ii. Furthermore, the data streams are divided equally throughout the devices by evaluating the connections load using an effective edge technique.
- iii. Using blockchain technology, the SDN controller lowers the degree of communication attacks and creates a trustworthy environment. It increases the reliability of the data diffusion process in unpredictable circumstances.
- iv. To assess the performance of DFTDS under realistic conditions, several simulation-based tests are performed.

The remaining part of this research work is organized in the following sections. Section II discusses the literature and identifies the problem statement. Section III explains the methodology for the DFTDS in detail. The system model and simulations are conducted in Section IV with the analysis of various experiments. Section V concludes this research study.

II. RELATED WORK

IoT system allows smart devices to perceive and interact with the real world and communicate with each other [23-25]. Urban applications are embedded with sensors, actuators, visual cameras, and cloud services to monitor traffic control, surveillance, and smart home automation using IoT systems [26, 27]. Furthermore, they make it possible to cope with timely remote monitoring of the surveillance system by incorporating security techniques [28-30]. Authors in [31] developed an effective rapid subspace deconstruction over Chi Square

transformation for smart city surveillance-based IoT. Local binary pattern histogram extracts video classification information. Fast subspace decomposition over Gaussian distributed Local Binary Pattern (LBP) features removes superfluous features. Battery-powered surveillance systems use more memory and time due to this redundancy. Because of improved feature reduction, the suggested approach works for all image identification applications in IoT-based surveillance equipment. Well-known databases validate the suggested approach. Raspberry Pi implementation yields excellent outcomes for all databases. In [32], a reliable and energy-efficient sector-based forwarding method for data packet routing in underwater wireless sensor networks is proposed. Sector-based forwarding ensures secure and reliable data routing. The proposed network model divides the network into sectors to optimize hop count and data delivery. By maintaining a sector-by-sector sequence through the pivot node, known as the sector head, the data forwarding mechanism is carried out vertically. In [33], authors presented a secure approach for choosing Cluster Heads (CHs) based on nodes' trust value called Trust Aware Clustering Technique for WSN-based Intelligent Transportation System (TACTIRSO). To effectively choose CHs, the proposed approach used the Rat Swarm Optimizer (RSO), a more modern swarm-based optimization technique. The proposed fitness function considers the trust value and node remaining energy for choosing CH. In addition, the predefined threshold values are changed dynamically following the network state using the exponential moving average approach. It also employed a variety of local search approaches in addition to an energy-efficient and trust-aware initialization strategy for the rat population, which enhances RSO performance.

Authors [34] proposed a Lightweight Task Scheduling and Routing Optimizing alternative for RPL (L2RMR) with a new Objective Function (OF) and a path route minimization routine measure. A Stochastic Process prevented the overall Herd Decampment Phenomenon (HDP) issue. The proposed technique delays parent joining for nodes to obtain a lower rank instead of greedy thundering, causing network topology instability. The Contiki-Cooja simulator assessed L2RMR performance. L2RMR was tested under different networking sizes, data rates, and densities. In RPL and other similar scenarios, they improved the average packet loss ratio, end-to-end delay, and energy consumption. A decentralized security architecture based on SDN and blockchain technology for smart city IoT networks was proposed to detect attacks [35]. SDN, Blockchain, Fog, and mobile edge computing are the three leading technologies in the proposed architecture. SDN continuously monitors and analyzes traffic data in the IoT network to provide an optimal attack detection model. Moreover, blockchain provides decentralized attack detection to address the "single point of failure" issue. In [36], authors proposed and analyzed a novel fair and distributed congestion control strategy for Neighborhood Area Networks (NANs). The major goal is to ensure fair network access by preventing high-traffic nodes from controlling channels. Moreover, traffic flows from various applications have been prioritized. The objective is to offer all traffic flows the necessary service quality, particularly during periods of heavy traffic load. The concept is evaluated within a wireless ad hoc network comprising various

smart grid metering devices. Machine learning techniques can potentially extract patterns for identifying and classifying security threats. Accordingly, the authors in [37] proposed an intrusion detection system (IDS) for identifying flooding attacks in vehicle-related scenarios. Using the Network Simulator 3 (NS-3), the proposed solution modeled 5G-enabled vehicle scenarios and created different datasets with various node counts, attacker densities, and mobility patterns with Simulation of Urban Mobility (SUMO) support.

Compared to existing systems, the performance results show an improved classification of flooding attacks. In [38], the authors proposed a Reliable Multipath Routing Protocol based on Link Quality and Stability in Urban Areas (RMQS-ua). It is a multi-path routing solution to ensure reliable data transmission with the consideration of optimal link quality and connectivity. To assess network quality, it combines the signal-to-noise ratio (SNR), the enhanced packet reception ratio (PRR), and the exponential moving average (EMA). Simulation results revealed the improved performance of RMQS-ua in terms of network metrics than existing solutions.

Based on the related work, IoT networks and edge technologies are quickly influencing the development of smart applications, especially in urban environments. The connected devices can collect the necessary data and play a vital role in remote areas. Researchers have developed a variety of route-aware techniques that facilitate the prompt response for critical applications. However, controlling a data flow on network channels is a significant research challenge. Most present solutions cannot adapt quality-aware metrics while achieving optimal routing consequences. In addition, when developing the cooperative solution, it is important to consider the misuse of sensitive data along with stable access to IoT resources.

III. SMART TRAFFIC FLOWING WITH HETEROGENEOUS TECHNOLOGIES FOR SECURED SMART CITIES

This section explains the discussion of the smart and distributed data fault-tolerant protocol with the integration of SDN architecture. The DFTDS consists of three distinct phases. In the first phase, the IoT sensors, neighbors, and links are identified and recorded their information to edge devices. The edge devices are deployed to cope with additional overheads on the devices and increase the timely delivery of critical urban data. The SDN controllers manage and control the edge devices for the efficient performance of IoT technologies with limited computing capacity on the devices. Moreover, hash enabled blockchain scheme provides a trusted connection to ensure the protection and authentication of shared data.

A. OPTIMIZED DATA CONTROLLING WITH NOMINAL COMPLEXITY

In the beginning, edge devices send the request packets in their transmission range to gather the information of the nearest nodes. When collecting the data, they store it in their memory and refresh it whenever new events are generated. This is the continuous method for edge devices to maintain the lower layer intelligently. The lower layer comprises mobile sensors N , wireless channels WC , gateway devices, GD . Later, by exploring the collaborative strategies, the nodes initiate the transmission system for forwarding the observing data with the least communication cost. Cost computation which manages devices and intelligently controls traffic is the main component

of DFTDS. The DTFDS protocol utilizes the greedy local optimizing technique to follow the most reliable and delay-aware routing paths. Accordingly, it reaches an optimal global decision by computing local optimal iterations. We assumed that WC is composed of various links as given in Equation 1.

$$WC = (L_1, L_2, L_3, \dots, L_n) \quad (1)$$

Each link has an associated cost value and is computed each time to update the records at edge devices. DTFDS identified feasible solutions FS for connections L_n based on specified criteria. Let us consider that FS is comprised of $(S_1, S_2, S_3, \dots, S_n)$ such that each solution is selected after analyzing a set of criteria. Later, to forward the IoT data, the DTFDS protocol determines the optimal solution Opt_s from the S_i using the minimum cost function, as stated in Equation 2.

$$Opt_s = \min.cost(S_i) \quad (2)$$

The local optimal solution LOS , which eventually leads to a globally optimal solution, is computed using the minimal cost function. The decision is based on the number of hop counts HP_c , packet arrival rate PK_a and overload factor OL_f . Equation 3 defines the summation with minimized cost.

$$\min(LOS) = HP_c + PK_a + OL_f \quad (3)$$

PK_a is computed by determining the time consumed based on exploring arriving $A(tm)$ and sending time $S(tm)$ of data packets, as defined in Equation 4.

$$PK_a = A(tm) - S(tm) \quad (4)$$

OL_f depends on the ratio of packets lost. As demonstrated in Equation 5, the forwarding channel is overloaded if the ratio of lost packets Pk_l exceeds threshold T , and the routing flag r_i for the existing route is set to false.

$$\begin{aligned} & \text{if } Pk_l > T \\ & \text{then } r_i = \text{false} \end{aligned} \quad (5)$$

The parameters that have been declared in the equations are presented in Table I.

TABLE I
DECLARED PARAMETERS

Parameter	Description
N	Sensor nodes
WC	Wireless channels
GD	Gateway devices
L_n	Data links
FS	Feasible solution
Opt_s	Optimal solution
HP_c	Hop count
PK_a	Packet arrival rate
OL_f	Overload factor
$A(tm)$	Arrival time
$S(tm)$	Sending time
Pk_l	Lost packets
T	Threshold

r_i	Routing flag
SC	Security code
N_i	Edges
Id	Identity
$+$	Exclusive OR
mk	Chunks of messages
$h(m_i)$	Message hash

B. SECURED COMMUNICATION PARADIGM WITH CENTRALIZED SDN COMPUTATION

SDN controllers manage resources and support long-term IoT network-edge device communication. All the edge devices make their entries in the controller mapping tables. When an edge device cannot handle massive IoT data flow, the SDN controller removes it from the edge boundary and introduces a new suitable node as an edge device. Edge devices have a distinct mapping table identifier, and each time the SDN controller examines the identity of the edge device. If verification is successful, the SDN controller sends data to the cloud system; otherwise, it drops it. For authentication, identity Id and generated nonce of the edge device N_i are combined and obtain a unique security code SC , as given in Equation 6.

$$SC = Id + N_i \quad (6)$$

where $+$ operation shows the xor function. On the other hand, the SDN controller utilized the nonce N_i that is generator by edge device and performs xor operation with obtained SC value, as stated in Equation 7.

$$Id = SC + N_i \quad (7)$$

After confirming edge devices, the DTFDS protocol examines the hashes for message chunks mk and interconnects, as shown in Equation 8.

$$H(M) = h(m1) + h(m2) + \dots + h(mk) \quad (8)$$

Figure 1 shows the three DFTDS stages. In the first stage, different tiers have been identified. In the low-level tier, IoT sensors collaborate to build local structures. In the middle-level tier, IoT sensors are forwarding their data toward edge devices, and in the high-level tier, edge devices are in contact with SDN controllers. Later, the source node generates a route request and makes local and global optimal decisions based on defined criteria. Finally, the SDN controller authenticates edge devices and forwards data in blockchain mode.

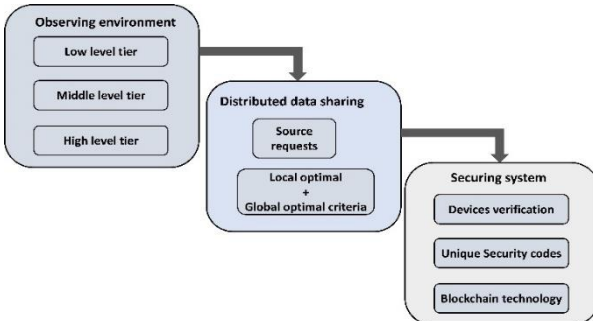


Figure 1. Proposed phases of DFTDS

Figure 2 and Figure 3 show the flowcharts of the DFTDS for traffic management in heterogeneous networks and security against non-authorized access. The source node routes sensor data to edge devices and provides the local optimum solutions for maintaining distributed systems. This approach is repeated until the globally optimum solution is found. When traffic flows are determined and nodes are overloaded, the DFTDS removes the communication links from the mapping tables. And, later the updated information is stored in the SDN controller. Moreover, security is achieved with the centralized approach by using an SDN controller. Edge devices are verified based on the security computing and once they are declared authentic, their data is acceptable to SDN controllers.

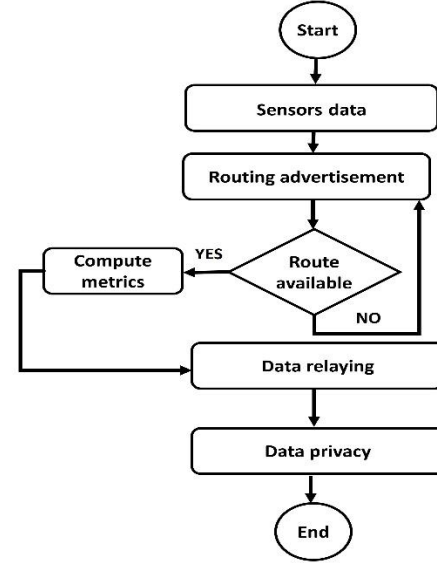


Figure 2. DFTDS for heterogeneous intelligent data flowing

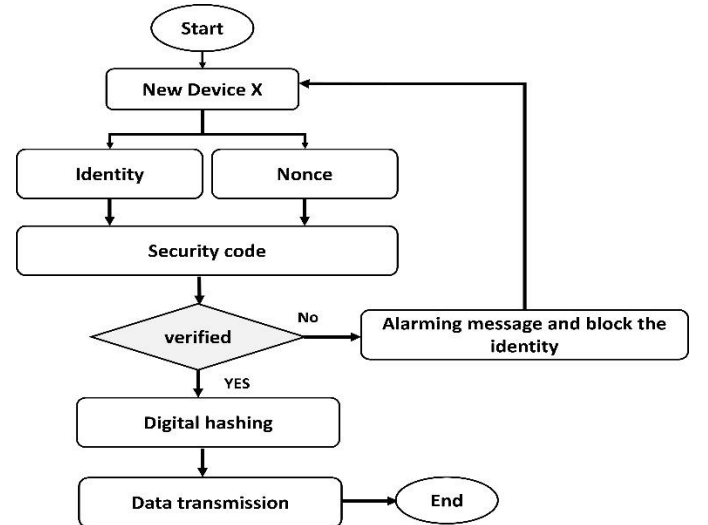


Figure 3. DFTDS for security in a communication system

IV. SIMULATION ENVIRONMENT AND ANALYSIS OF RESULTS

This section explains the NS-3 simulation environment and analyzes the results. Multiple experiments are evaluated by utilizing mobile sensors and edge nodes. Mobility patterns were recorded at specific intervals of 5s to 10s from the data trace

files. These network trace data include the most recent device location, traveled distance, and movement speed. Ultimately, the DFTDS analyses this data to make intelligent traffic management decisions. The neighboring tables are updated by exploring certain events. We used 2 SDN controllers with adequate resources in comparison to the other devices. Both the low-level layer and the high-level tier are accessible to edge devices. The performance is evaluated based on two scenarios i.e. varying time from 10 min to 50 min and varying malicious nodes from 2 to 10. The DFTDS is tested against TACTIRSO [33] and L2RMR [34]. The simulation parameters are presented in Table II.

TABLE II
SIMULATION PARAMETERS

Parameter	Value
Simulation area	1000m X 1000m
Mobile Sensors	30, 50, 70, 90, 110
Number of sinks	3
Initial energy	1j to 3j
Mobility pattern	5s to 10s
Data packets	2000 bits/sec
Data traffic	CBR
Transmission range	2m
SDN controller	2
Simulations	30
Malicious nodes	2-10
Simulation time	10 min to 50 min
Performance metrics	Packet delivery, network latency, link disconnection network complexity, and alive nodes

A. DISCUSSION

According to Figures 4(a) and 4(b), the DFTDS improved the performance of packet delivery in terms of varying time and malicious nodes. Packet delivery is the ratio of total packets delivered to total packets sent from the source node to the destination node over the network system. The experimental results demonstrate an 8.3% and 11.6% improvement for the DFTDS compared to other work. It uses local and globally optimal solutions until end-to-end communication links are identified. Moreover, the updated parameters in collaborative criteria balance the consumption of network resources and ultimately efficiently utilize the communication bandwidth. Furthermore, edge nodes perform a key role in the DFTDS, as they are intermediate devices nearest to the low-level tier and shorten the network routes accordingly. Such practice increases the delivery of IoT data with the least interruption. By utilizing the security solution, the data chunks are forwarded with trusted forwarders, reducing the chances for malicious packets to affect the actual nodes' communication. The DFTDS and alternative solution are simulated regarding nodes overhead against varying time and malicious nodes. Figures 5(a) and 5(b) show that the DFTDS reduces link disconnection by an average of 7.7% and 10.2% compared to existing techniques. It is defined as a link breakage rate while sending and receiving the data packets over the network system. The DFTDS initiates collaborative criteria for building an alternate route when traffic on forwarding routes exceeds a particular limit. With edge

support, SDN monitors the network field and significantly reduces link damage even with malicious nodes. Exploring nonce and unique node identifications allows security techniques to find defective nodes rapidly. Thus, the DFTDS ensures smooth transmission over IoT channels.

Figures 6(a) and 6(b) depicted the efficacy of the DFTDS in comparison to existing solutions for varying time and malicious nodes in terms of network latency. It can be defined as the time the network takes to send packets from the source end to the destination. Observations indicate that the DFTDS reduces the latency factor by an average of 10.6% and 14.1% compared to the existing work. This is due to the low-level devices' collaborative decision-making and record-keeping services. In addition, route requests are generated only when data forwarding is required. The congested channels are identified intelligently, and data is shared in traffic-aware routes.

Consequently, the DFTDS reduces both the frequency of retransmissions and the latency time on IoT networks. Moreover, only the most recent information is maintained at the edges and longer routes are eliminated from the tables. This allows for rapid packet transmission from a source node toward edge nodes using an optimized selection of neighboring nodes. The performance of the DFTDS and an alternative solution is simulated in terms of network complexity, as shown in Figures 7(a) and 7(b). It depends on constructing alternative routes and coping with packet disturbance over the communication system. Even if the number of malicious nodes increases, the DFTDS reduces communication breakages by 7.6% to 12.4% on average. The neighbors' list is kept up-to-date by analyzing hop count and traffic flow data, thus increasing the efficiency of communication bandwidth. Using the threshold limit, the DFTDS first determined whether a particular route is appropriate for transmitting IoT data. If the decision is not optimal, it investigates alternative data transmission routes by balancing the overheads on the nodes.

Moreover, the DFTDS's authentication methods reduce the possibility of data anomalies, resulting in the lowest communication cost in data aggregation and analysis at network edges. In terms of alive nodes, Figures 8(a) and 8(b) displayed the performance results of the DFTDS compared to existing solutions under varied time intervals and malicious nodes. Compared to existing work, the DFTDS algorithm improves the ratio of alive nodes by an average of 13.3% and 15.8% respectively. This is due to the low-level devices' collaborative decision-making and record-keeping of various communication metrics. By exploring the intelligent and distributed routing methods the overloaded transmission paths are identified and eliminated from stored information. Consequently, devices balance the additional energy dissipation in data retransmission and enhance the network node's stability. Moreover, peer-to-peer connections are re-established when the optimized criteria are not met. The security mechanisms used in DFTDS also reduce the possibility of malicious nodes issuing error messages, resulting in a longer network lifetime in terms of alive nodes.

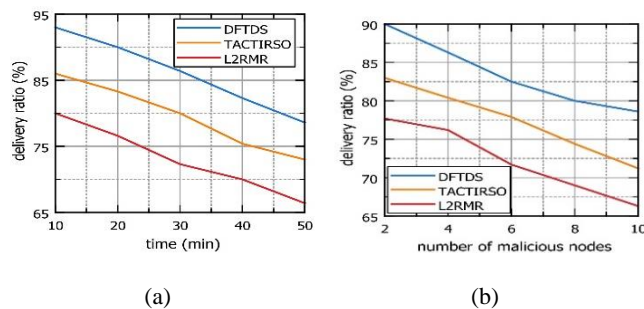


Figure 4. Evaluation of packet delivery under (a) varying time from 10 to 50 min (b) varying malicious nodes from 2 to 10.

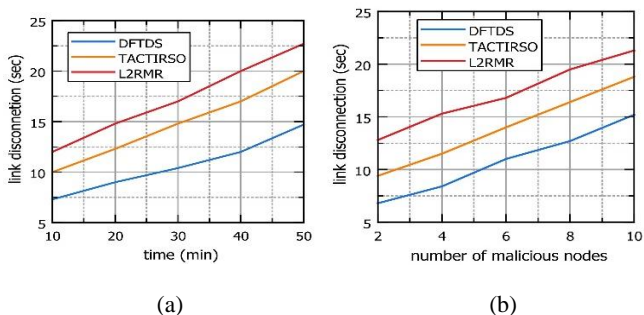


Figure 5. Evaluation of link disconnection under (a) varying time from 10 to 50 min (b) varying malicious nodes from 2 to 10.

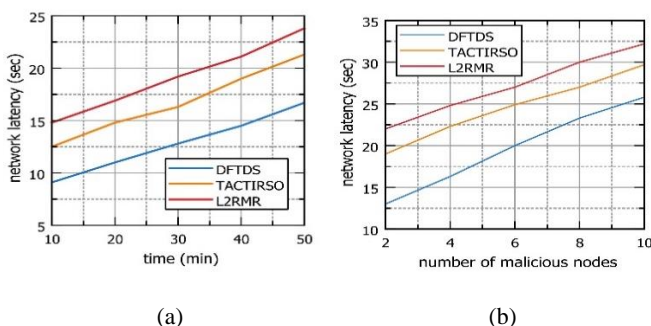


Figure 6. Evaluation of network latency under (a) varying time from 10 to 50 min (b) varying malicious nodes from 2 to 10.

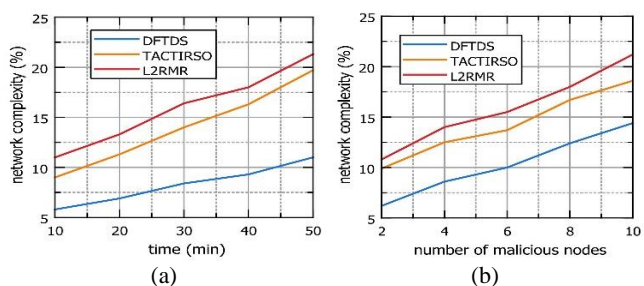


Figure 7. Evaluation of network complexity under (a) varying time from 10 to 50 min (b) varying malicious nodes from 2 to 10

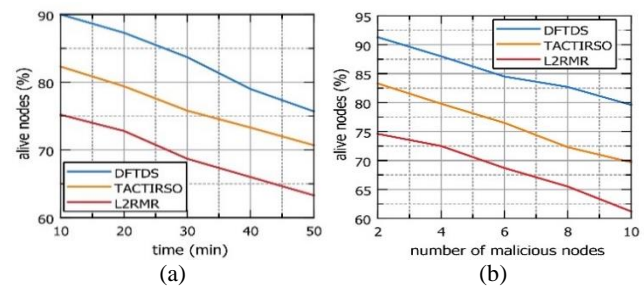


Figure 8. Evaluation of alive nodes under (a) varying time from 10 to 50 min (b) varying malicious nodes from 2 to 10

V. CONCLUSION

Heterogeneous networks comprise many sensors, IoT systems, and wireless equipment for collecting a huge amount of data in urban applications. The heterogeneous nodes gather varied data types and facilitate the smart application to access and further analyze the information. Homogeneous communication systems provide a lot of potential solutions, but their resource limitations and ineffective use of cooperative decision-making present several research challenges. In urban areas, wireless communication also poses security risks and compromises data integrity. This study presents an SDN controller-enabled secured data-sharing solution for heterogeneous traffic management. Using cooperative greedy algorithms, real-time data of urban sensing systems is transmitted toward the edges. In addition, edges maintain records for neighbors in proximity and share valuable data with the network system to control the data distribution process. Blockchain technologies are being investigated to achieve hash-enabled security in terms of privacy and verification. Performance findings show that the DFTDS performs significantly better than previous work in terms of delivery ratio, delay rate, network complexity, link disconnection, and number of alive nodes. However, it was discovered that the machine learning strategy might further enhance the data fusion procedure with minimal computational power for devices. In the future, we would like to incorporate the concept of federated learning with realistic public data sets to develop the intrusion detection system.

FUNDING

This research was funded by Princess Nourah bint Abdulrahman University and Researchers Supporting Project number (PNURSP2023R346), Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia

ACKNOWLEDGEMENT

This research was supported by the Artificial Intelligence & Data Analytics (AIDA) Lab CCIS Prince Sultan University, Riyadh, Saudi Arabia. The authors are thankful for their support.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

REFERENCES

1. Talebkhah, M., et al., *IoT and big data applications in smart cities: recent advances, challenges, and critical issues*. IEEE Access, 2021. **9**: p. 55465-55484.
2. Kumari, A., R. Gupta, and S. Tanwar, *Amalgamation of blockchain and IoT for smart cities underlying 6G communication: A comprehensive review*. Computer Communications, 2021. **172**: p. 102-118.
3. Tawalbeh, L.a., et al., *IoT Privacy and security: Challenges and solutions*. Applied Sciences, 2020. **10**(12): p. 4102.
4. Haseeb, K., et al., *Trust management with fault-tolerant supervised routing for smart cities using internet of things*. IEEE Internet of Things Journal, 2022. **9**(22): p. 22608-22617.
5. Jiang, J.C., et al., *Federated learning in smart city sensing: Challenges and opportunities*. Sensors, 2020. **20**(21): p. 6230.
6. Bera, S., S. Misra, and A.V. Vasilakos, *Software-defined networking for internet of things: A survey*. IEEE Internet of Things Journal, 2017. **4**(6): p. 1994-2008.
7. Yang, F., et al., *A survey on multisource heterogeneous urban sensor access and data management technologies*. Measurement: Sensors, 2022. **19**: p. 100061.
8. Popović, I., et al., *Building low-cost sensing infrastructure for air quality monitoring in urban areas based on fog computing*. Sensors, 2022. **22**(3): p. 1026.
9. Musaddiq, A., Y.B. Zikria, and S.W. Kim, *Routing protocol for Low-Power and Lossy Networks for heterogeneous traffic network*. EURASIP Journal on Wireless Communications and Networking, 2020. **2020**(1): p. 1-23.
10. El-Fouly, F.H., et al., *ERCP: Energy-Efficient and Reliable-Aware Clustering Protocol for Wireless Sensor Networks*. Sensors, 2022. **22**(22): p. 8950.
11. Gures, E., et al., *A comprehensive survey on mobility management in 5G heterogeneous networks: Architectures, challenges and solutions*. IEEE Access, 2020. **8**: p. 195883-195913.
12. Mohammadi, M., et al., *Deep learning for IoT big data and streaming analytics: A survey*. IEEE Communications Surveys & Tutorials, 2018. **20**(4): p. 2923-2960.
13. Ghahramani, M., M. Zhou, and G. Wang, *Urban sensing based on mobile phone data: Approaches, applications, and challenges*. IEEE/CAA Journal of Automatica Sinica, 2020. **7**(3): p. 627-637.
14. Sarker, I.H., *Smart City Data Science: Towards data-driven smart cities with open research issues*. Internet of Things, 2022. **19**: p. 100528.
15. Jan, M.A., et al., *An AI-enabled lightweight data fusion and load optimization approach for Internet of Things*. Future Generation Computer Systems, 2021. **122**: p. 40-51.
16. Sada, A.B., et al. *A distributed video analytics architecture based on edge-computing and federated learning*. in 2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech). 2019. IEEE.
17. Shah, N., H. El-Ocla, and P. Shah, *Adaptive Routing Protocol in Mobile Ad-hoc Networks using Genetic Algorithm*. IEEE Access, 2022.
18. He, S., et al., *Multi-source reliable multicast routing with QoS constraints of NFV in edge computing*. Electronics, 2019. **8**(10): p. 1106.
19. Haseeb, K., et al., *LSDAR: A Light-weight Structure based Data Aggregation Routing Protocol with Secure Internet of Things Integrated Next-generation Sensor Networks*. Sustainable Cities and Society, 2019: p. 101995.
20. Al-Turjman, F., H. Zahmatkesh, and R. Shahroze, *An overview of security and privacy in smart cities' IoT communications*. Transactions on Emerging Telecommunications Technologies, 2022. **33**(3): p. e3677.
21. Nguyen, V.-L., et al., *Security and privacy for 6G: A survey on prospective technologies and challenges*. IEEE Communications Surveys & Tutorials, 2021. **23**(4): p. 2384-2428.
22. Nguyen, D.C., et al., *Blockchain for 5G and beyond networks: A state of the art survey*. Journal of Network and Computer Applications, 2020. **166**: p. 102693.
23. Kumar, S., P. Tiwari, and M. Zymbler, *Internet of Things is a revolutionary approach for future technology enhancement: a review*. Journal of Big data, 2019. **6**(1): p. 1-21.
24. Hang, L. and D.-H. Kim, *Design and implementation of an integrated iot blockchain platform for sensing data integrity*. Sensors, 2019. **19**(10): p. 2228.
25. Islam, N., et al., *Secured Protocol with Collaborative IoT-Enabled Sustainable Communication Using Artificial Intelligence Technique*. Sustainability, 2022. **14**(14): p. 8919.
26. Atlam, H.F. and G.B. Wills, *IoT security, privacy, safety and ethics*, in *Digital twin technologies and smart cities*. 2020, Springer. p. 123-149.
27. Gupta, B.B. and M. Quamara, *An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols*. Concurrency and Computation: Practice and Experience, 2020. **32**(21): p. e4946.
28. Hamdan, S., M. Ayyash, and S. Almajali, *Edge-computing architectures for internet of things applications: A survey*. Sensors, 2020. **20**(22): p. 6441.
29. Tabrizchi, H. and M. Kuchaki Rafsanjani, *A survey on security challenges in cloud computing: issues, threats, and solutions*. The journal of supercomputing, 2020. **76**(12): p. 9493-9532.
30. Rahouti, M., K. Xiong, and Y. Xin, *Secure software-defined networking communication systems for smart cities: current status, challenges, and trends*. IEEE Access, 2020. **9**: p. 12083-12113.
31. Kumar, M., et al., *An efficient framework using visual recognition for IoT based smart city surveillance*. Multimedia Tools and Applications, 2021. **80**(20): p. 31277-31295.
32. Kumar, R., et al., *EESR: Energy efficient sector-based routing protocol for reliable data communication in UWSNs*. Computer Communications, 2022. **192**: p. 268-278.
33. Osamy, W., et al., *TACTIRSO: trust aware clustering technique based on improved rat swarm optimizer for WSN-enabled intelligent transportation system*. The Journal of Supercomputing, 2023. **79**(6): p. 5962-6016.
34. Seyfollahi, A. and A. Ghaffari, *A lightweight load balancing and route minimizing solution for routing protocol for low-power and lossy networks*. Computer Networks, 2020. **179**: p. 107368.
35. Rathore, S., B.W. Kwon, and J.H. Park, *BlockSecIoTNet: Blockchain-based decentralized security architecture for IoT network*. Journal of Network and Computer Applications, 2019. **143**: p. 167-177.
36. León, J.P.A., et al., *A fair and distributed congestion control mechanism for smart grid neighborhood area networks*. Ad Hoc Networks, 2020. **104**: p. 102169.
37. Sousa, B., N. Magaia, and S. Silva, *An Intelligent Intrusion Detection System for 5G-Enabled Internet of Vehicles*. Electronics, 2023. **12**(8): p. 1757.
38. Benatia, S., et al., *A reliable multipath routing protocol based on link quality and stability for MANETs in urban areas*. Simulation Modelling Practice and Theory, 2021. **113**: p. 102397.

Amjad Rehman is a senior researcher in the Artificial Intelligence & Data Analytics Lab CCIS Prince Sultan University Riyadh Saudi Arabia. He received his PhD & Postdoc from Faculty of Computing Universiti Teknologi Malaysia with a specialization in Forensic Documents Analysis and Security with honor in 2010 and 2011 respectively. He received rector award for 2010 best student in the university. Currently, he is PI in several funded projects and also completed projects funded from MOHE Malaysia, Saud Arabia. His keen interests are in Data Mining, Health Informatics, Pattern Recognition. He is author of more than 200 ISI journal papers, conferences and is a senior member of IEEE.

Khalid Haseeb did a Ph.D. in Computer Science from the Faculty of Computing, Universiti Teknologi Malaysia (UTM), Malaysia in 2016. He has an experience of several years in teaching, research, and development He is a Postdoctoral fellow in the Artificial Intelligence & Data Analytics (AIDA) research lab at CCIS Prince Sultan University, Riyadh, Saudi Arabia. His research areas include wireless sensor networks, ad-hoc networks, network security, artificial intelligence, machine learning, software-defined networks, and cloud computing. He is involved as a referee for many reputed international journals and conferences.

Teg Alam, Ph.D., is presently working as a faculty member at the Industrial Engineering Department, College of Engineering, Prince Sattam Bin Abdulaziz University, Al Kharj; Kingdom of Saudi Arabia. Before joining Prince Sattam Bin Abdulaziz University, he worked at Azad Institute of Engineering and Technology, U.P. Technical University Lucknow, India, as an Associate Professor. His areas of teaching and research interests are Operations Research, Quantitative Analysis, and Applied Statistical Methods. He has published numerous researches in different reputed peer-reviewed scientific journals.

Faten S. Alamri received a Ph.D. degree in system modeling and analysis in statistics from Virginia Commonwealth University, USA, in 2020. Her Ph.D. research was in Bayesian dose response modeling, experimental design, and nonparametric modeling. She is currently working as an Assistant Professor with the Department of Mathematical Sciences, College of Science, Princess Nourah Bint Abdul Rahman University. Her research interests include spatial area, environmental statistics, and brain imaging.

Tanzila Saba is a full professor & leader of AIDA Lab CCIS Prince Sultan University Riyadh KSA. Her primary research focus in recent years is medical imaging, MRI analysis, and Soft-computing. She has two hundred ISI/SCEI publications that have around 4000 citations with h-index 40. Her mostly publications are in biomedical research published in ISI/SCIE indexed. Due to her excellent research achievement, she is included in Marquis Who's Who (S & T) 2012." Currently, she is an editor and reviewer of reputed journals and on the panel of TPC of international conferences. She has full command of a variety of subjects and taught several courses at the graduate and postgraduate levels. On the accreditation side, she is a skilled lady with ABET & NCAAA quality assurance. She is the senior member of IEEE. Dr. Saba is the leader of the Artificial Intelligence & Data Analytics Lab.

Houbing Song (M'12–SM'14–F'23) received the Ph.D. degree in electrical engineering from the University of Virginia, Charlottesville, VA, in August 2012. He is currently a Tenured Associate Professor, the Director of the NSF Center for Aviation Big Data Analytics (Planning), the Associate Director for Leadership of the DOT Transportation Cybersecurity Center for Advanced Research and Education (Tier 1 Center), and the Director of the Security and Optimization for Networked Globe Laboratory (SONG Lab, www.SONGLab.us), University of Maryland, Baltimore County (UMBC), Baltimore, MD. Prior to joining UMBC, he was a Tenured Associate Professor of Electrical Engineering and Computer Science at Embry-Riddle Aeronautical University, Daytona Beach, FL. He serves as an Associate Editor for IEEE Transactions on Artificial Intelligence (TAI) (2023-present), IEEE Internet of Things Journal (2020-present), IEEE Transactions on Intelligent Transportation Systems (2021-present), and IEEE Journal on Miniaturization for Air and Space Systems (J-MASS) (2020-present). He was an Associate Technical Editor for IEEE Communications Magazine (2017–2020). He is the editor of eight books, the author of more than 100 articles and the inventor of 2 patents. His research interests include cyber-physical systems/internet of things, cybersecurity and privacy, and AI/machine learning/big data analytics. His research has been sponsored by federal agencies (including National Science Foundation, US Department of Transportation, and Federal Aviation Administration, among others) and industry. His research has been featured by popular news media outlets, including IEEE GlobalSpec's Engineering360, Association for Uncrewed Vehicle Systems International (AUVSI), Security Magazine, CXOTech Magazine, Fox News, U.S. News & World Report, The Washington Times, and New Atlas. Dr. Song is an IEEE Fellow, an ACM Distinguished Member, and an ACM Distinguished Speaker. Dr. Song has been a Highly Cited Researcher identified by Clarivate™ (2021, 2022) and a Top 1000 Computer Scientist identified by Research.com. He received Research.com Rising Star of Science Award in 2022 (World Ranking: 82; US Ranking: 16). Dr. Song was a recipient of 10+ Best Paper Awards from major international conferences, including IEEE CPSCoM-2019, IEEE ICII 2019, IEEE/AIAA ICNS 2019, IEEE CBDCoM 2020, WASA 2020, AIAA/ IEEE DASC 2021, IEEE GLOBECOM 2021 and IEEE INFOCOM 2022.