ISSN: 2182-2069 / E-ISSN: 2182-2077

A Trust-based Security and Privacy Protection for Data Collection in Smart City

Dr. Arasu Raman[1*], Dr. Anantha Raj Arokiasamy[2], Chitra Batumalai[3], Dr. Mudiarasan Kuppusamy[4], Dr. Rajani Balakrishnan[5], and Dr. Stephen Antoni Louis[6]

[1*]Faculty of Business and Communications, INTI International University, Malaysia.
arasu.raman@newinti.edu.my, https://orcid.org/0000-0002-8281-3210

[2]Faculty of Business and Communications, INTI International University, Malaysia.
anantharaj.asamy@newinti.edu.my, https://orcid.org/0000-0001-9784-6448

[3]Faculty of Data Science and Information Technology, INTI International University, Malaysia.
chitra.batumalai@newinti.edu.my, https://orcid.org/0009-0003-2001-5605

[4]Tun Razak Graduate School, University Tun Abdul Razak, Malaysia.
arasan@unirazak.edu.my, https://orcid.org/0000-0003-0502-2455

[5]Faculty of Business and Communications, INTI International University, Malaysia.
rajani.balakrishnan@newinti.edu.my, https://orcid.org/0000-0002-0467-2053

[6]Faculty of Management Sciences, Knowledge Institute of Technology, India.
directorkbs@kiot.ac.in, https://orcid.org/0009-0002-4421-1830

Received: February 21, 2024; Revised: April 15, 2024; Accepted: May 27, 2024; Published: August 30, 2024

Abstract

Ensuring the genuineness and reliability of the data collected at the data collecting stage is of utmost importance in the Smart City (SC) industrial ecosystem. They influence the precision of statistical analysis and the impartiality of decision-making. Identifying attack behaviors caused by external interference and establishing a secure data transmission channel for terminals with limited resources are complex challenges. This paper presents a solution to these issues by introducing a Trust-based Security System (TSS). Within the framework of TSS, the initial step involves creating a trust model that utilizes binomial distribution to calculate the trust value of each node. The research implements a third-party suggestion method to enhance the objective of the trust rating. The research provides a trust management strategy to mitigate the ON-OFF assault. The study develops a robust routing algorithm that effectively manages the trade-off between safety, transmission effectiveness, and energy consumption. A comprehensive simulation exercise assesses the analytical findings of the TSS.

Keywords: Security, Privacy, Data Collection, Sustainable Building, Smart City.

1 Introduction to Security Issues in Smart City

A Smart City (SC) is a spatial environment that combines physical, online, and social structures to create interconnected networks and activities (Kirimtat et al., 2020). The purpose is to optimize the use of

Journal of Internet Services and Information Security (JISIS), volume: 14, number: 3 (August), pp. 18-28.
DOI: *10.58346/JISIS.2024.I3.002*

*Corresponding author: Faculty of Business and Communications, INTI International University, Malaysia.

resources, enhance engagement with government officials, and promote the overall welfare of its inhabitants. A SC is a metropolitan region that utilizes existing physical structures and various methods, including the Internet of Things (IoT), physical relationships, cyber systems, networked sensors, and details and communication technology (Priyanka et al., 2023). By collecting data from different neighborhoods and conducting a thorough analysis, a SC aims to enhance the housing surroundings, continually improve the quality of life, stimulate financial and social growth, foster equitable growth and environmental protection, optimize energy resource utilization, enhance the efficiency of urban structures, address local issues, and facilitate more effectively urban planning (Lee et al., 2021; Alamer & Shadadi, 2023). An SC is not limited to the use of mechanical or electronic devices. The research encompasses political dedication, social funding, and the active involvement of residents. These factors are crucial in implementing sustainable and inclusive remedies that enhance the safety and resilience of cities. Implementing systemic solutions, such as cybersecurity rules and ethical data management requirements, can significantly improve SC residents' quality of life and confidence, advancing the SC idea. Alongside the numerous advantages that the concept of an SC provides, it is crucial to tackle and analyze the broader array of obstacles and potential hazards that its implementation presents for authorities, institutions, organizations, and prospective service providers.

The advancement of digital protection systems is closely associated with sustainable technological advancement (Rolim et al., 2021). The safety of SC citizens can be compromised by threats such as data abuse or intrusions of their digital privacy. These incidents can result in a lack of trust in the services offered and a negative view of the SC idea. Public policy plays a crucial role in deciding the level and accuracy of data that citizens of smart cities are prepared to provide.

Numerous sensor nodes and smart devices are placed in unattended locations, such as water quality detectors for ecological security, geomagnetic detectors in intelligent transport, and illumination detectors in the innovative street light network. When the gathered and combined sensed data are transmitted to the gateways or base station across a public wireless channel, there is a risk that an adversary intercepts or manipulates the data. These inaccurate data will significantly impact the precision of statistical analysis and the impartiality of decision-making. An intelligent sensor's computational and storage capacity is restricted, preventing the deployment of advanced security methods (Ballard et al., 2021). Ensuring the genuineness and completeness of collected data is a significant obstacle.

During the data gathering phase, smart terminals employ algorithms for encryption with low computing cost or lightweight identification techniques to defend against external assaults such as eavesdropping, jamming assaults, and Denial of Service (DoS) assaults (Vinh et al., 2023; Chaganti et al., 2022). While these efforts enhance security to a certain degree, they do not effectively address the issue of internal attacks, such as data discarding, manipulating, replaying, or forgeries. These types of attacks pose a more significant threat to the network.

2 Background and Related Works

Many sensing devices produce a substantial volume of information, and intelligent networks must analyze and handle the vast quantities of data created by these devices to enhance network efficiency (Surendar et al., 2024). The research provides sophisticated tactics to improve network efficiency and deliver top-notch services to users. This data frequently includes a substantial quantity of sensitive information. The research imposes stricter safety standards for the IoT.

Javaid et al., integrated sensing devices with mobile vehicles (Javaid et al., 2021). They implemented a reward system determined by the distance the automobile covers. The price is calculated by considering just the distance traveled by the automobile and the extent of city covering. Liu et al., suggest a framework for recruiting vehicles based on trajectory, considering both the accessibility of vehicles in space and time and the reputation of participants (Liu et al., 2020). The goal is to recruit vehicles to accomplish the specified geographical coverage while staying within a specific budget.

Yang et al., introduced a vehicle recruiting method aimed at maximizing the level of data collection by providing vehicles with incentives to participate in data collecting (Yang et al., 2022). Hartmann et al., introduced a sophisticated assessment system that relies on mobile edge computing (Hartmann et al., 2022). They developed a probabilistic graphical framework to guarantee the reliability of nodes and minimize energy usage. Chiejina et al., suggested using the beta function as a likelihood density measure to assess the trustworthiness of nodes (Chiejina et al., 2022). Mo et al., suggested including a distinct hash value at the intermediary node during packet forwarding, uniformly evaluating the hashed value of the intermediary node at the final node, and adjusting the trust counter based on the verified outcome (Mo et al., 2020).

Feng et al., introduced a trust evaluation technique that utilizes crowdsourcing and innovative mobile computer systems (Feng et al., 2020). Portable edge users can acquire a range of data and assess the reliability of a node by being physically close to the terminal nodes. Srilakshmi et al., suggested employing a reliable base station to regularly gather and verify packets from nearby nodes, ensuring the safety of the routing pathway (Srilakshmi et al., 2021). Zagrouba & Kardi contend that the engaged mechanism necessitates initiating paths to test different nodes, which the research results in the consumption of extra energy (Zagrouba & Kardi, 2021). Mohamed et al., suggested an innovative data-gathering technique that combines Unmanned Aerial Vehicles (UAVs) with mobility vehicles to minimize data collection delays (Mohamed et al., 2020).

Adnan et al., introduced a two-step safe authentication system for multiplexed Mobile Ad Hoc Network (MANET) (Adnan et al., 2022). The system could effectively defend against ON-OFF attacks, where rogue nodes had a specific ambush period to squander system assets intentionally. The detection time for these attacks was unexpected. Gao et al., introduced a new routing method that is both safe and reliable, considering many constraints (Gao et al., 2020). This algorithm is designed to be Quality-of-Service (QoS) conscious and is based on the Ant Colony Optimization (ACO) approach. Its main objective is to ensure a secure and resilient route. Simulation findings showed that the suggested routing method could find viable routes and ensure the efficient delivery of data packets. However, more research is needed to examine the impact of altruism on adopting electric cars from the standpoint of pro-environmental behavior (Raman & Ramachandaran, 2023).

Many obstacles arise during the data-collecting stage, such as constrained energy resources, lost packets, and security concerns. Developing a safe routing protocol necessitates the careful consideration of several issues. A practical and secure routing system represents a tradeoff between security and availability for interfaces with limited resources.

3 Proposed Trust-based Data Collection Model in Smart City

3.1. Smart City Model

Figure 1: Sample Structure of the Smart City

The network model, seen in Figure 1, is built and comprises sensing gadgets, data-gathering tools, and data centres. In a SC, various urban facilities, such as street lamps and garbage bins, are fitted with sensor devices to monitor their surroundings. These devices possess uncomplicated equipment and a limited communication range of tens of meters. The sensors can utilize their restricted computational capacity to save information temporarily. When an Internet-connected Data-Collecting Tool (DCT) comes within range of these sensors, the information is transmitted from the devices to the portable DCT. The data is sent to a sophisticated data center using DCT. Mobile vehicles (MVs) and UAVs are DCTs in several research studies that satisfy the customer experience (Raman et al., 2023). The data produced by the detectors will be taken in and preserved by the data-gathering tool. The data acquired by the UAVs will undergo additional processing in a data center. This process will include activities such as trust evaluation, recruiting of MVs, incentives, and decision-making in the Logistics Industry (Prashanth et al., 2024). Specific sophisticated data centers can deploy UAVs.

3.2. Problem Statement

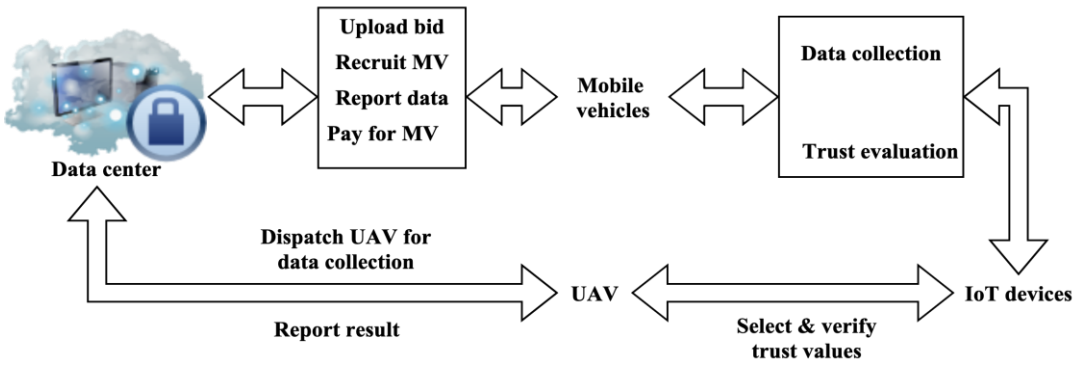


Figure 2: Layered data Collection Model

Figure 2 depicts the arrangement of data collecting using a layered trust method. The centralized data center employs mobile vehicles to gather information, which is then obtained by the vehicles' sensors. The trust level of the terminating nodes is calculated and sent to the data center. The UAV is deployed to actively assess the reliability of the nodes and automobiles in the network at a suitable moment and

transmit this information to the data center. The data center consolidates the information provided and assesses the trustworthiness of the sustainable circular business network (Khalife et al., 2024). MVs are compensated appropriately. To assure accuracy, the cloud thoroughly computes the sensor node multiple times with various cars, producing the final assessment result. The suggested technique can gather data from the networks. It calculates the trust evaluation of every individual node in the system and determines the reliability of the mobile vehicles.

3.3. System Overview

The assurance of the genuineness and unaltered state of the collected data is accomplished by eliminating any hostile nodes and carefully choosing a safe next hop. The TSS framework has three key elements: the Binomial Distribution (BD), the ON-OFF Trust Management Mechanism (OOTMM), and the Trust-based Secured Routing Algorithm (TSRA). Blockchain technology is a crucial and superior trust paradigm that provides a more impartial television experience. This TV utilizes OOTMM to safeguard against ON-OFF attacks and implements TSRA to transfer the collected data securely. Figure 3 provides a comprehensive overview of the framework.

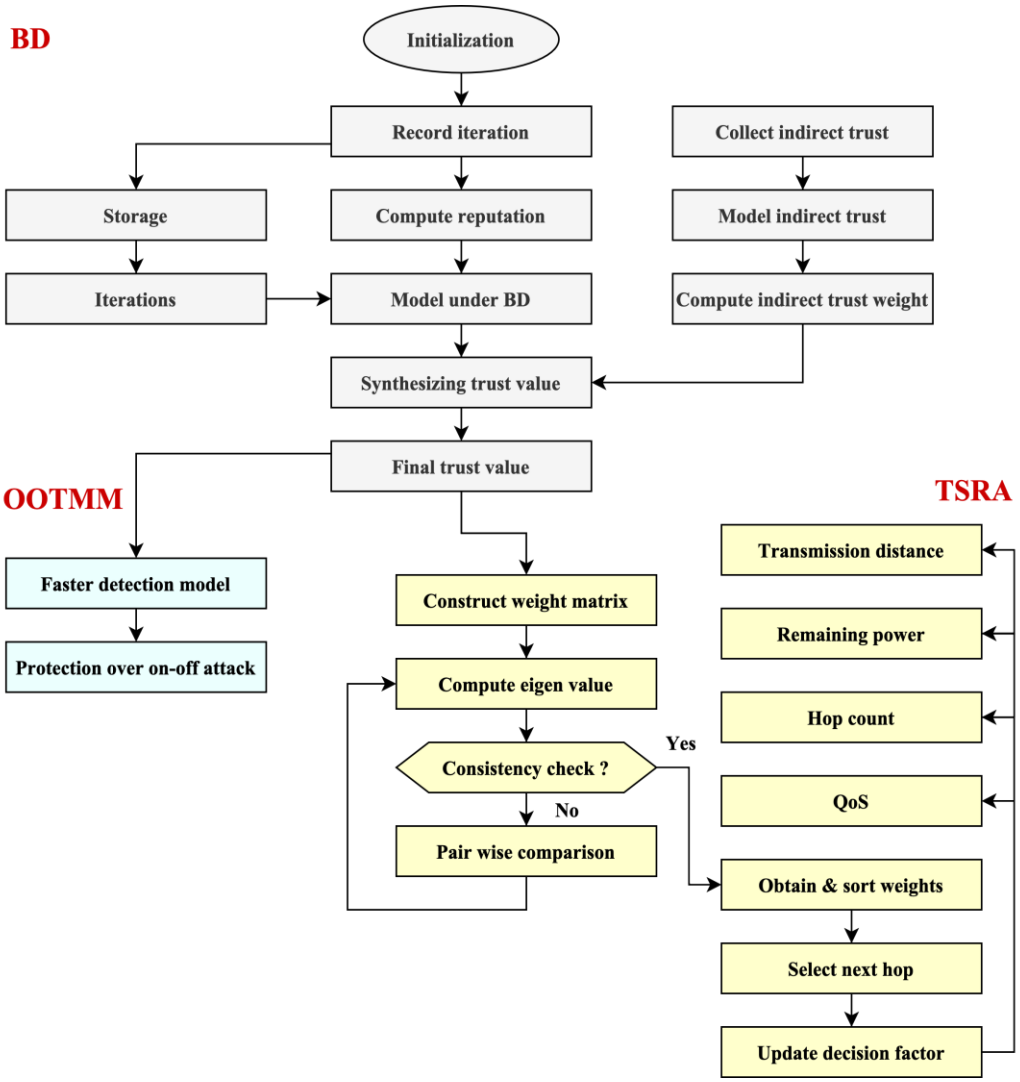


Figure 3: Architectural Overview of the Proposed System

3.4. Trust Model by Using BD

A trust model often denotes a structured approach for building, assessing, and overseeing trust in relationships between different organizations. This research provides a trust framework that uses binomial transportation, characterized by a series of n independent Bernoulli trials. The collaboration or noncooperation of the relationships among the networks determines the efficacy or otherwise of each Bernoulli trial. The likelihood distribution functional represents the trustworthiness of one sensor node towards a different sensor node, reflecting a reciprocal trust connection between the two networks. Either cooperation or noncooperation continually maintains it, using knowledge management and big data analytics capabilities (Subrahmanyam et al., 2024).

The BD is a probabilistic probability that primarily describes the distribution of discontinuous occurrences, often consisting of two distinct occurrences (Sulaiman et al., 2022). The beta distribution is a continuum probability distribution specified inside the interval (0, 1). The link between the two probabilities above is that the binary dispersion represents the beta dispersion when n equals 1. Given the limited computational complexities and storage capacity, this approach only records and calculates the amount of collaboration and noncooperation using binomial dissemination. This method is appropriate for representing and quantifying the interacting behaviors among resource-constrained detector nodes.

4 Simulation Analysis and Outcomes

The MATLAB software is used to model the BD and OOTMM in various application situations, while the NS-2 software is used to simulate the TSRA. In BD and OOTMM, the variables a and b are taken to have a value of 5, and the trust value is set to an initial value of 0.5. The research assumes the existence of a shared neighboring node, denoted as k.

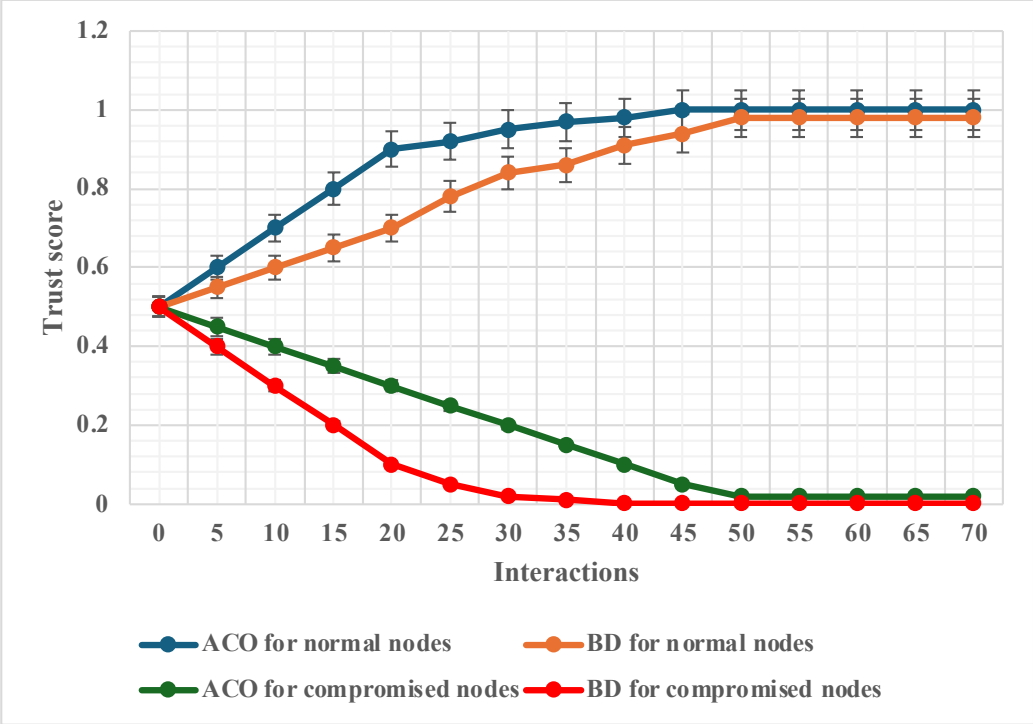


Figure 4: Trust Score Analysis

In Figure 4, the trust score in BD and ACO exhibits a boost when there is an increase in cooperative actions during interaction. When comparing ACO to BD, the trust score in BD can achieve far lower levels. When node j gets hacked and the level of noncooperation increases, the trust score will steadily fall and finally reach zero. The television market in BD is seeing a more rapid decline than ACO's. The study results indicate that BD is more in line with the trust principle of "difficult to acquire, easy to lose" than ACO.

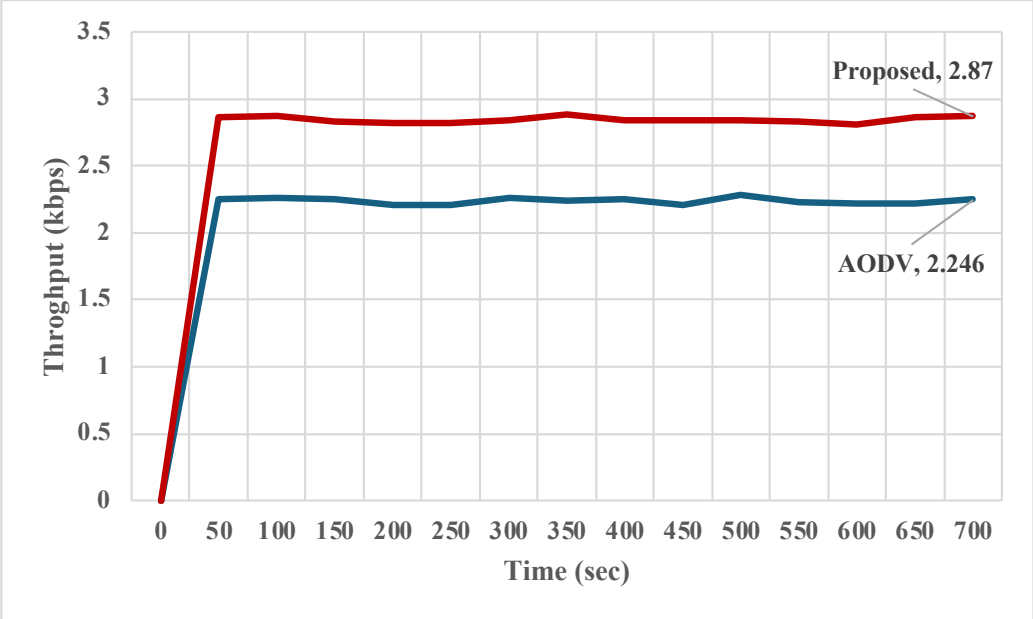


Figure 5: Throughput Analysis

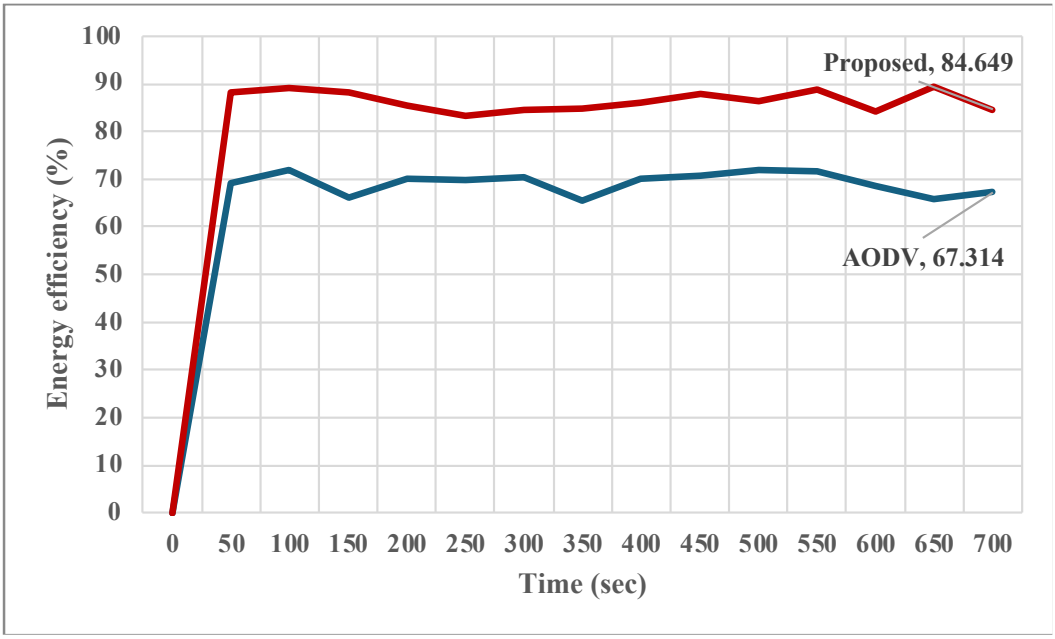


Figure 6: Energy Efficiency Analysis

Figures 5 and 6 demonstrate a well-established correlation between throughput and energy consumption. As the number of effectively delivered data packets by the routing protocol grows, energy

utilization in the research improves accordingly. The simulation findings demonstrate that introducing the trust score for decision-making enables it to retain a comparable level of network performance. The proposed system ensures security by implementing hash chains and digital signatures. The energy utilization will increase as the encrypting overhead grows. TSRA employs television as a security measure rather than relying on intricate encryption methods. While TSRA has lower energy consumption than the traditional Adhoc On-demand Distance Vector (AODV) routing algorithm, it effectively preserves the internal safety of the system and guarantees its smooth functioning. TSRA has successfully created a harmonious equilibrium between security, usage of energy, and transmission efficiency.

5 Conclusion and Findings

Gathering data in a SC industrial context poses an enormous obstacle regarding confidentiality. The collected data must be consolidated and delivered instantly, ensuring authenticity and integrity concurrently. It is crucial to comprehend the efficient design of a security system that can withstand assaults within a terminal with limited resources. It is essential to promptly detect non-cooperative behaviors caused by external interferences in a complex urban setting.

A TSS was developed to ensure the security of data collecting. The things the research does are unique and innovative for the following reasons.

1. A trust approach was presented by incorporating a third-party suggestion into the binomial distribution-based approach. An adjustable indirect credibility weight was developed in BD to enhance the objectivity of the ultimate TV and account for the energy usage balancing.
2. OOTMM was presented to address the time-varying features of the wireless channel while gathering data and the attack behaviors during ON-OFF attacks. It does this by analyzing the propagation of the shifting pattern of TV.
3. A secured routing system was designed with the choice factors. The system can choose the most suitable and secure next-hop node for transmitting the collected data while maintaining a balance between security, cost-effectiveness, and transmission effectiveness.

Simulation analysis showed that the BD can better fulfill the trust principle's criteria of being "difficult to obtain, but easy to lose." The OOTMM can promptly and efficiently identify and protect against ON-OFF attacks. The TSRA was able to strike a balance between safety, transmission effectiveness, and energy consumption. In the future, the primary objective will be to enhance the ability to identify and safeguard against internal assaults by implementing trust management projects and integrating TSRA into various networks.

References

[1] Adnan, M. H., Ahmad Zukarnain, Z., & Harun, N. Z. (2022). Quantum key distribution for 5g networks: A review, state of the art and future directions. *Future Internet, 14*(3), 73. https://doi.org/10.3390/fi14030073

[2] Alamer, L., & Shadadi, E. (2023). DDoS Attack Detection using Long-short Term Memory with Bacterial Colony Optimization on IoT Environment. *Journal of Internet Services and Information Security, 13*(1), 44-53.

[3] Ballard, Z., Brown, C., Madni, A. M., & Ozcan, A. (2021). Machine learning and computation-enabled intelligent sensor design. *Nature Machine Intelligence, 3*(7), 556-565.

[4] Chaganti, R., Boppana, R. V., Ravi, V., Munir, K., Almutairi, M., Rustam, F., & Ashraf, I. (2022). A comprehensive review of denial of service attacks in blockchain ecosystem and open challenges. *IEEE Access*, *10*, 96538-96555.

[5] Chiejina, E., Xiao, H., Christianson, B., Mylonas, A., & Chiejina, C. (2022). A robust Dirichlet reputation and trust evaluation of nodes in mobile ad hoc networks. *Sensors*, *22*(2), 571. https://doi.org/10.3390/s22020571

[6] Feng, W., Yan, Z., Yang, L. T., & Zheng, Q. (2020). Anonymous authentication on trust in blockchain-based mobile crowdsourcing. *IEEE Internet of Things Journal*, *9*(16), 14185-14202.

[7] Gao, H., Liu, C., Li, Y., & Yang, X. (2020). V2VR: reliable hybrid-network-oriented V2V data transmission and routing considering RSUs and connectivity probability. *IEEE Transactions on Intelligent Transportation Systems*, *22*(6), 3533-3546.

[8] Hartmann, M., Hashmi, U. S., & Imran, A. (2022). Edge computing in smart health care systems: Review, challenges, and research directions. *Transactions on Emerging Telecommunications Technologies*, *33*(3), e3710. https://doi.org/10.1002/ett.3710.

[9] Javaid, M., Haleem, A., Rab, S., Singh, R. P., & Suman, R. (2021). Sensors for daily life: A review. *Sensors International*, *2*, 100121. https://doi.org/10.1016/j.sintl.2021.100121

[10] Khalife, D., Subrahmanyam, S., & Farah, A. (2024). A Sustainable Circular Business Model to Improve the Performance of Small and Medium-sized Enterprises Using Blockchain Technology. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA)*, *15*(2), 240-250.

[11] Kirimtat, A., Krejcar, O., Kertesz, A., & Tasgetiren, M. F. (2020). Future trends and current state of smart city concepts: A survey. *IEEE Access*, *8*, 86448-86467.

[12] Lee, H., Jung, S., & Kim, J. (2021). Distributed and autonomous aerial data collection in smart city surveillance applications. *In IEEE VTS 17th ASIA pacific wireless communications symposium (APWCS)*, 1-3.

[13] Liu, L., Wen, X., Wang, L., Lu, Z., Jing, W., & Chen, Y. (2020). Incentive-aware recruitment of intelligent vehicles for edge-assisted mobile crowdsensing. *IEEE Transactions on Vehicular Technology*, *69*(10), 12085-12097.

[14] Mo, W., Wang, T., Zhang, S., & Zhang, J. (2020). An active and verifiable trust evaluation approach for edge computing. *Journal of Cloud Computing*, *9*, 1-19.

[15] Mohamed, N., Al-Jaroodi, J., Jawhar, I., Idries, A., & Mohammed, F. (2020). Unmanned aerial vehicle applications in future smart cities. *Technological Forecasting and Social Change*, *153*, 119293. https://doi.org/10.1016/j.techfore.2018.05.004

[16] Prashanth, B. Arasu, R., & Karunanithy, D. (2024). Perceptual Study on Higher Level Digitalization Among Managers in the Logistics Industry. *The Journal of Distribution Science*, *22*(1), 25-36.

[17] Priyanka, J., Ramya, M., & Alagappan, M. (2023). IoT Integrated Accelerometer Design and Simulation for Smart Helmets. *Indian Journal of Information Sources and Services*, *13*(2), 64–67.

[18] Raman, A., & Ramachandaran, S. D. (2023). Factors Influencing Consumer's Adoption of Electric Cars in Malaysia. *TEM Journal*, *12*(4), 2603-2612.

[19] Raman, A., Suhartanto, D., & Shaharun, M.H.B. (2023). Delightful Customer Experience: An Antecedent for Profitability and Sustainable Growth of Airline Businesses. https://doi.org/10.20944/preprints202312.1838.v1

[20] Rolim, F. B., Trindade, F. C., & Rider, M. J. (2021). Adaptive protection methodology for modern electric power distribution systems. *Journal of Control, Automation and Electrical Systems*, *32*(5), 1377-1388.

[21] Srilakshmi, U., Veeraiah, N., Alotaibi, Y., Alghamdi, S. A., Khalaf, O. I., & Subbayamma, B. V. (2021). An improved hybrid secure multipath routing protocol for MANET. *IEEE Access*, *9*, 163043-163053.

[22] Subrahmanyam, S., Aishwaryalaxmi, N. S., Khalife, D., Shaikh, I. A. K., Faldu, R., & Asthana, N. (2024). Impact of Knowledge Management and Big Data Analytics Capabilities on Firm Performance. *In Ninth International Conference on Science Technology Engineering and Mathematics (ICONSTEM)*, 1-5.

[23] Sulaiman, N. S., Fauzi, M. A., Wider, W., Rajadurai, J., Hussain, S., & Harun, S. A. (2022). Cyber–information security compliance and violation behaviour in organisations: A systematic review. *Social Sciences*, *11*(9), 386. https://doi.org/10.3390/socsci11090386.

[24] Surendar, A., Saravanakumar, V., Sindhu, S., & Arvinth, N. (2024). A Bibliometric Study of Publication - Citations in a Range of Journal Articles. *Indian Journal of Information Sources and Services*, *14*(2), 97–103. https://doi.org/10.51983/ijiss-2024.14.2.14

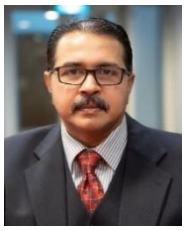
[25] Vinh, D.T., Phi, T.L., & Viet, C.T. (2023). A Secure Proxy Re-Signature Scheme for IoT. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications*, *14*(1), 174-188.

[26] Yang, X., Gu, B., Zheng, B., Ding, B., Han, Y., & Yu, K. (2022). Toward incentive-compatible vehicular crowdsensing: An edge-assisted hierarchical framework. *IEEE Network*, *36*(2), 162-167.

[27] Zagrouba, R., & Kardi, A. (2021). Comparative study of energy efficient routing techniques in wireless sensor networks. *Information*, *12*(1), 42. https://doi.org/10.3390/info12010042

Authors Biography

Dr. Arasu Raman a senior lecturer in Marketing and Management at INTI International University, holds a Ph.D. in Business Administration with a specialization in Marketing. With over 27 years of teaching experience, he is certified as a Professional Trained Teacher by the University of Hertfordshire and in Case Teaching by Harvard Business School. Dr. Arasu has published 26 research articles on entrepreneurship, digital marketing, and marketing information systems. He is renowned for his innovative curricula and collaborations with multinational companies.



Dr. Anantha Raj Arokiasamy an Associate Professor at INTI International University, has over 20 years of experience in educational leadership and management in Malaysia's private higher education institutions. With a bachelor's degree in business administration, Master of Arts in International Business, MBA, and Ph.D. in Educational Management and Leadership, he has authored books and published over 80 academic papers, influencing global educational policy and leadership development initiatives.

Chitra Batumalai is a senior lecturer at INTI International University, specializing in Data Science and Information Technology. With a background in programming and IBM modules, she has made significant contributions to teaching and research. With a MIS from Coventry University and an MBA from Inti University, she is known for her commitment to quality education and innovative approach in Information and Technology.

Professor Dr. Mudiarasan Kuppusamy is currently a Professor at University Tun Abdul Razak, specialing in supervision of doctoral candidates. He has been working in academics and research for more than 20 years with end-to-end knowledge in digital strategy and solutions for small and medium-sized enterprises. He is a skilled data modeler and analyst with a specialism in Information, Communication & Technologies. Prof Dr. Mudiarasan is experienced in defining roadmaps & strategies and people management for numerous organizations in Malaysia. In 20 years, he has been part of several educational institutions, namely the University of Cyberjaya, Asia Pacific University, Monash University Malaysia, and Western Sydney University, Australia. He is also a passionate trainer in the field of digital environment, exclusively data privacy.

Dr. Rajani Balakrishnan a Ph.D. in Mobile Technology, has over 20 years of teaching experience in higher learning institutions. She specializes in integrating mobile technologies into education, enhancing learning outcomes. Balakrishnan has shaped curricula that bridge technology and education, fostering innovation. She is a leader in educational technology and has mentored numerous students.

Dr. Stephen Antoni Louis is a highly experienced academician and corporate professional with over 25 years of experience. He is the Director of the MBA program at Knowledge Institute of Technology, Salem, and holds multiple qualifications, including a Ph.D., MBA, M.A, M.Phil, and a Six Sigma Green Belt from Benchmark. Dr. Stephen has served in leading institutions and has been an approved research supervisor for Anna University, Chennai.