sustainability

MDPI

Article

Energy-Efficient Mobile Agent Protocol for Secure IoT Sustainable Applications

Mohamed Elhoseny [1,2,*], Mohammad Siraj [3], Khalid Haseeb [4,*], Muhammad Nawaz [5], Majid Altamimi [3] and Mohammed I. Alghamdi [6]

1 Faculty of Computers and Information, Mansoura University, Mansoura 35516, Egypt
2 College of Computing and Informatics, University of Sharjah, Sharjah 27272, United Arab Emirates
3 Electrical Engineering Department, College of Engineering, King Saud University, Riyadh 11421, Saudi Arabia; siraj@ksu.edu.sa (M.S.); mtamimi@ksu.edu.sa (M.A.)
4 Department of Computer Science, Islamia College Peshawar, Peshawar 25000, Pakistan
5 Department of Computer Science, Institute of Management Sciences, Peshawar 25000, Pakistan; m.nawaz@imsciences.edu.pk
6 Department of Computer Science, Al-Baha University, Al-Baha 1988, Saudi Arabia; mialmushilah@bu.edu.sa
* Correspondence: melhoseny@ieee.org (M.E.); khalid.haseeb@icp.edu.pk (K.H.)

Abstract: The Internet of Things (IoT) and sensor technologies are combined with various communication networks in smart appliances and perform a significant role. Connected devices sense, analyze, and send environmental data, as well as support applications' connections. Mobile agents can be explored to provide sensing intelligence with IoT-based systems. Many strategies have been proposed to address the issue of energy efficiency while maintaining the sensor load at a low cost. However, advancements are still desired. Furthermore, without fully trustworthy relationships, sensitive data are at risk, and the solution must provide privacy protection against unexpected events. With the development of two algorithms, this study proposes a mobile agent-based efficient energy resource management solution and also protects IoT appliances. Firstly, the software agents perform a decision using past and present precepts, and by exploring rule-based conditions, it offers an energy-efficient recommended system. Second, data from IoT appliances are securely evaluated on edge interfaces before being transferred to end-centers for verification. Simulations-based tests are conducted and verified the significance of the proposed protocol against other studies in terms of network metrics.

Keywords: Internet of Things; network management; sustainable applications; agents; mutual trust

Citation: Elhoseny, M.; Siraj, M.; Haseeb, K.; Nawaz, M.; Altamimi, M.; Alghamdi, M.I. Energy-Efficient Mobile Agent Protocol for Secure IoT Sustainable Applications. *Sustainability* **2022**, *14*, 8960. https://doi.org/10.3390/su14148960

Academic Editor: Zubair Baig

Received: 24 May 2022
Accepted: 18 July 2022
Published: 21 July 2022

1. Introduction

Internet of Things (IoT) is now widely used in many critical applications for advanced development such as smart buildings, surveillance security, target tracking, industrial automation, etc. [1–3]. On the other side, the wireless sensor network (WSN) and multi-agents are also gaining rapid popularity due to their dynamic structure, as well as offering smart services with minimum energy [4,5]. Such networks are comprised of low-cost sensor nodes with limited computing, communication, memory, and power capabilities. Moreover, agents move between nodes to collect data and decrease the communication overheads for ordinary sensors [6–8]. Such technologies are one of the many viable data sources since large-scale networks of sensor nodes produce a massive amount of big data. In mobile agent-based routing, either single or multi-agents are distributed from the sink node to the source node for collecting environmental data. Such practices not only increase the performance for data aggregation but, on the other side, also balance the traffic load on the routes with an improved network lifetime [9,10]. Unlike typical wireless networks [11–13], WSNs have substantial data dependability and communication challenges due to node limitations. When a dense sensor of nodes is used, a large proportion of the data collected is irrelevant, worthless, or redundant [14,15]. Many machine-learning-based approaches

have been presented to overcome the data gathering and routing problems in constraint networks, and significantly decrease the data disturbance for critical applications [16–18]. However, massive data are created with the advent of IoT networks, and it is necessary to bring cloud characteristics closer to the request generator so that enormous data may be processed closer to the end-user [19–21]. Providing storage and processing at the network edge minimizes network traffic and eliminates several cloud computing problems. In addition, the architecture of fog computing aids big data processing and the efficient usage of resources. A cloud-based platform is sometimes referred to as a big data warehouse and supports real-time event processing [22–24]. Real-time data access is necessary for critical and sustainable applications with manageable and efficient communication flow. Furthermore, a large number of computing edge devices that are located closer to the sink node demanded high computing requirements with low latency by exploring some learning models [25,26]. Moreover, it is observed that real-time data from IoT sensors should be available to remote devices with mutual trust and hidden patterns to increase reliability in edge-based networks [27,28]. It is noticed that a few systems are capable of providing intelligent communication models based on mobile edge devices, including minimum data alteration and energy management [29–31]. Although edge networks provide reliable and timely data transmission for wireless technologies, they are vulnerable to network attacks and sensitive data compromise due to unwanted device association. As a result, this research proposed a mobile agent-based secured edge protocol for sustainable applications, intending to provide additional benefits to smart applications in terms of resource management, energy efficiency, bandwidth, and latency requirements, including privacy and data security.

The following contributions are made by this research work:

i. It offers a mobile agent-based collaborative routing solution that exploits fitness functions and selects the most optimal nodes for data aggregation services.
ii. The probability of the nodes for data routing is increased and it trains the proposed protocol using experiences to reduce its communication overheads.
iii. Mutual trust offers an authentic method using security tokens, and nodes are confident in sending their data to the mobile agents.
iv. Extensive experiments demonstrate the significant improvement of the proposed protocol for computing and resources management.

The remainder of the research study is organized as follows: The relevant work and formulation of the research challenges are highlighted in Section 2. Section 3 introduces the proposed protocol with its phases and flowcharts. Section 4 explains the experimental results and compares them to the relevant studies. Section 5 concludes with recommendations for future work.

2. Related Work

Smart things are proving to be advantageous for the development of IoT systems, as they efficiently manage wireless devices for sensing and transmitting data. Sustainable applications based on mobile agents are a promising alternative rather than a traditional communication system, as they collect the data from sensors, rather than relaying the data received by each node to the sink [32,33]. As a result, agents enabled the system to minimize energy consumption among the devices of IoT applications while also improving data relaying performance with the fewest overheads [34,35].

An energy-efficient MAC protocol was developed by authors [36] using reinforcement learning, a common artificial intelligence technique, and increases the network lifetime. The proposed protocol is built on Q-learning, which converges to a low energy state by repeatedly adjusting MAC settings through a process of trial and error. This solves the minimization problem without having to predetermine the system model and offers a self-adaptive protocol to topological and other external changes. Simulations-based results have proven their significance against existing work. The authors developed a SoftEdgeNet model [37] for a sustainable edge computing network, which is an SDN-based distributed

layered network architecture with the support of a blockchain approach. It handles the existing communication issues and adheres to architectural design principles. It also proposes an SDN-based secure fog node architecture at the fog layer to lessen security attacks and give real-time analytics services. The proposed model suggested a flow rule partition and allocation mechanism at the edge of the network. The evaluation's findings show that the proposed paradigm considerably enhances real-time data transmission exchanges. In [38], the authors divide industrial sensing data into three classes and prioritize them. To balance energy usage, it provides dependability and timeliness parameters, as well as builds a set of candidate nodes for data forwarding. After that, an energy-efficient and QoS-aware routing algorithm is developed, and various types of data can be transmitted using various strategies. Furthermore, the most critical industrial sensing data can be reliably and timely transferred to the sink node. All of these data are transferred to the most appropriate relay node if the data requirements for real-time reliability are met.

In [39], the authors proposed a Mobile-Agent Distributed Intelligence Tangle-Based Approach (MADIT), which is a feasible solution by using IOTA (Tangle). On two levels, MADIT enables dispersed intelligence. To begin, numerous mobile agents are used to handle node-level connections and collect low-level transaction data. Second, high-level intelligence handles transactions using a Tangle-based architecture. The proof-of-work offloads efficient processing and speed while minimizing energy depletion. Extensive testing has revealed that deploying mobile agents improves the transaction processing speed, resulting in increased scalability. The concept of mobile software agents is applied in [40] for the aggregation of IoT data. This research presents a unique mobile agent-based route planning technique for IoT data processing and transmission. There are two primary stages in the suggested solution. The first stage clusters IoT devices; the second stage arranges cluster-heads into groups using an angle-based technique for mobile agent assignment. The main goal of the second stage is to use the Markov Decision Process (MDP) to provide route planning for each mobile agent in each cluster-head group for efficient data aggregation. The proposed technique reduces energy usage, data transmission delay, and IoT reliability as compared to other related work.

According to the related studies, it is revealed that smart applications are exploring many wireless technologies with embedded sensors for information gathering. Such communication systems also collaboratively operate with multi-agents to reduce the transmission time and lower energy consumption. However, the management of data flow from source nodes toward the sink is a considerable research problem because of the intrinsic properties of a constraint network. Additionally, because of the enormous amount of data being collected, communication lines frequently become overloaded and lose data. Furthermore, edge boundaries have been shown to reduce delay performance for significant operations in a variety of domains; nevertheless, lowering sensors' energy consumption and maintaining intelligent control of trust are difficult goals to achieve.

3. Proposed Energy-Efficient Mobile Secured Agent Protocol

This section begins with a brief introduction of the proposed protocol, followed by a network model and its various phases. It consists of sensors, mobile agents, and a mobile sink. Agents migrate in their distance threshold and collectively gather the sensors' data and their parameters, and accordingly, the mobile agent stores the collected information in the agent table. We consider all the nodes have a different initial energy resource. The routing table is dynamic and only updates its entries whenever any external/internal events occur. Some nodes with high sensing, data aggregation, and transmission capabilities are selected for the role of cluster heads. All the mobile agents collaboratively interact with both the cluster heads and sink nodes. Figure 1 illustrates the developed components of the proposed protocol. It has three main components: Network construction, agents-based routing, and lightweight trust with security. During network construction, sensor nodes with agents are deployed in the observing field, and initially, neighboring nodes are identified by using a distance threshold. Furthermore, the sink is mobile and collaboratively

receives the data from agents. Agents migrate to the boundary of the node, and all the selected cluster transmit their data to the nearest agent. In the second component, the cluster heads are selected by exploring the values of the parameters and the probability of those nodes increasing whose cost value is retained within a preset threshold. The third component associates the mutual trust between agents and cluster heads, and accordingly, only verified data can be accessed by cloud users with the support security tokens.

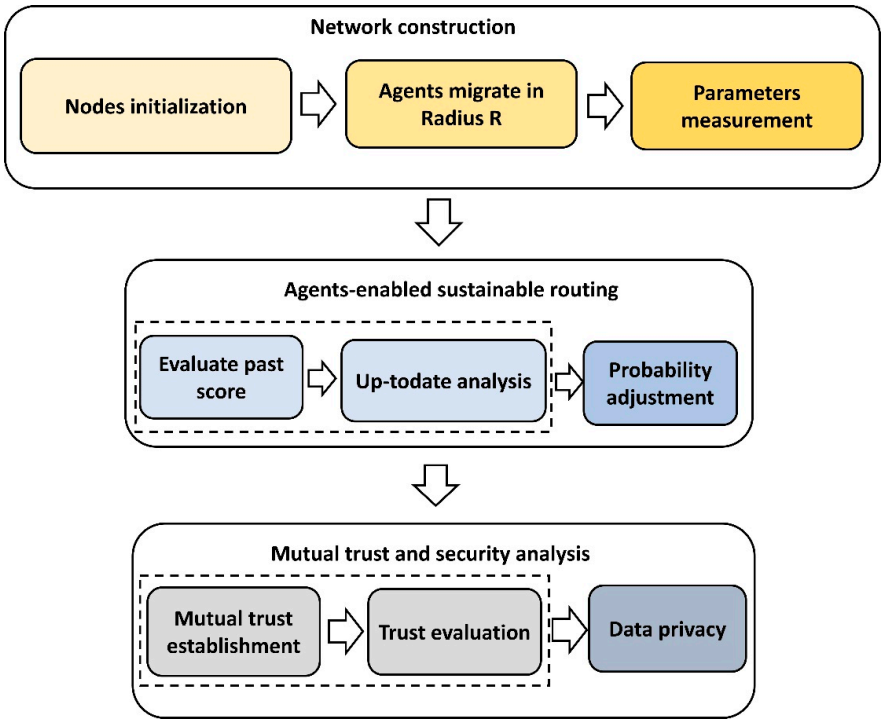


Figure 1. Developed components of the proposed protocol.

3.1. Mobile Agent-Based Optimal Routing

In this section, we present the discussion on the optimal routing in the mobile network by exploring agents. The agents are more intelligent than the cluster heads and serve as nodes' handlers. Based on the optimize function $f(i)$, the agent selects the cluster heads as denoted by X, such that the adjusted distance among them should be at least the preset threshold T, as given below.

$$D(x_i,\ x_j) < T;\ x_i,\ x_j\ \varepsilon\ X \tag{1}$$

The optimized function is the combination of the nodes' cumulative parameters value (v), including past experiences $f(i)'$ as defined below.

$$f(i) = c(v) + f(i)' \tag{2}$$

After the selection of cluster heads, the information on the selected ones is updated in the agent table, and the nearest nodes are the group in a form of a particular cluster. Whenever any changes are incurred in the agent table regarding nodes' parameters, the process of a new cluster head section is re-advertised. It may have happened that, at the time $t(i)$, if no node qualifies the optimal conditions for the cluster heads, then in such a case, the agent resumes the previous cluster head for data aggregation. The proposed protocol utilizes realistic parameters, such as residual energy $e(i)$, distance to agent $da(i)$, and error interval $err(i)$ for the determination of the $c(v)$ value, as given below.

$$c(v) = max(e(i),\ {}^{1}/_{da(i)},\ {}^{1}/_{err(i)}) \tag{3}$$

This process is repeated by an agent until the $c(v)$ value is maximized. Moreover, the error interval depends on the probability of lost packets p_α for time t as given below.

$$err(i) = p_\alpha / t + \sum_{i=0}^{n} di \tag{4}$$

where di is the summation of the delay rate in packets received from a source node. The mobile agents rotate around the formulated clusters and obtain the data by selected cluster heads. Additionally, the value of $c(v)$ is kept in the agent table and shared globally with other nodes. Let us consider that $\alpha_1, \alpha_2, \ldots\ldots, \alpha_k$ denotes the cost value for k sensors. After the computation of the cost value of a particular node i, and if it still falls in the preset threshold T, then its probability $P(i)$ for the selection of the cluster head is defined below.

$$P(i) = {}^{\alpha_i}/_{X};\ \alpha_i \geq T \tag{5}$$

3.2. Mutual Trust with Authentication and Privacy

The security of the agent-based sensor networks with mutual trust and authentication is discussed in this section. By examining agents' capabilities, the proposed protocol also addresses security threats from unexpected attacks. Each agent act as a middle-ware among sensors and the sink node. It not only ensures privacy and authentication but, on the other side, offers a trustworthiness system. Accordingly, all the nodes share their data with mutual trust. At the beginning, each agent x_i utilizes the security token S_t comprised of the pseudorandom number r_i and a timestamp. The token is encrypted using the session key k_i, as given below.

$$x_i \rightarrow n_i : S_t(r_i, timestamp) \oplus k_i \tag{6}$$

Upon receiving the security token, the cluster head n_i decrypts it using the same session key k_i, and recovers the r_i value. Afterward, the cluster head adds a random number r_j to the security token S_t, and sends the encrypted information to the agent x_i, as defined below.

$$n_i \rightarrow x_i : S_t(r_i, r_j, timestamp') \oplus k_i \tag{7}$$

Accordingly, both the associated agent and cluster head established mutual trust, and they can now transmit the data with a reliable and authentic communication source. In the case of a non-verifiable trust, the system generates an authentication error for the particular communication link. In addition, a new session key k_i' is generated for the transmission of data among the agent and cluster heads. The session key is forwarded by the agent to the cluster heads using an encryption layer based on asymmetric keys. When the newly generated session key is received by the sensor node, it will first recover it, and later, the privacy protection is achieved with the formation of the xor operation for data d_i, as given below.

$$E(d_i) = d_i \oplus k_i' \tag{8}$$

Finally, after proper authentication and security measurements, the data are forwarded from agents to the sink node and connected users can access the needed information. Table 1 depicts the meaning of all symbols.

Figure 2 demonstrates the flow chart of the proposed protocol. It is comprised of several procedures. Firstly, based on node conditions, the fitness function is evaluated. The nodes with maximum fitness value are declared as an initial cluster head. All the cluster heads are linked with the nearest agents, and the gathered data are transmitted toward the sink node. The routing phase performs a significant role in the IoT network, as the proposed protocol also computes the error ratio and decreases the chances for the selection of high-traffic data links. Moreover, the security tokens offer mutual trust among nodes and agents, which leads to reliable and authentic transmission systems. The robust and lightweight security analysis not only provides trustworthiness links but also ensures data privacy in the presence of threats. The cloud user can access the observing data from the sink node after verifying their identities.

Table 1. List of symbols.

Symbol	Meaning
$D(x_i, x_j)$	Distance between nodes
T	Preset threshold
X	Set of cluster heads
$f(i)$	Optimized function
$c(v)$	Commutative value
p_α	Lost packets
$e(i)$	Residual energy
$err(i)$	Error level
$da(i)$	Agent's distance
di	Delay rate
t	Time interval
E	Encryption
d_i	Data messages
$\oplus$	xor
k_i	Session key
k_i'	New session key
r_i, r_j	Random numbers

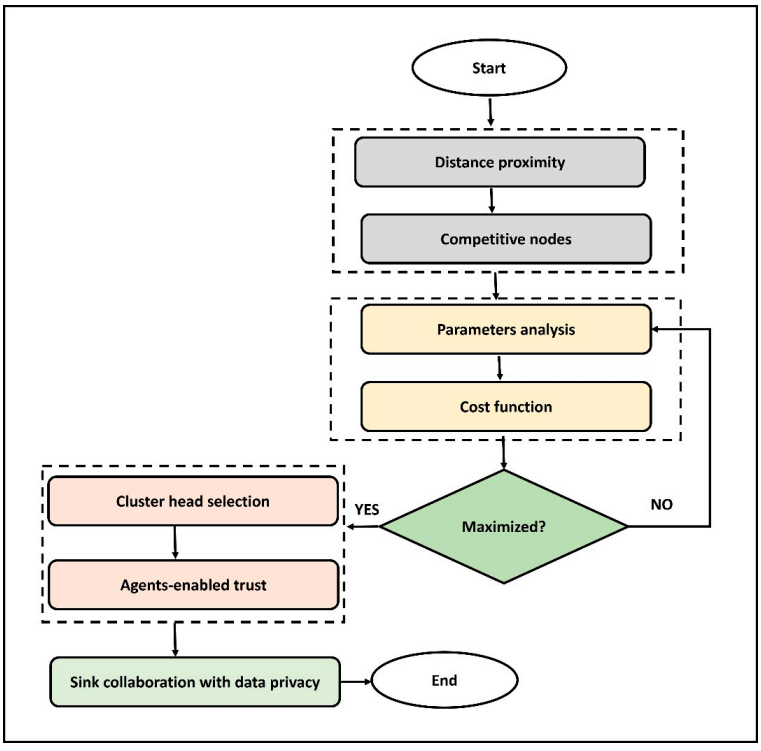


Figure 2. Flowchart of the proposed protocol.

4. Simulations

This section discusses the performance outcomes and the details of the experimental design. Simulations are used to examine and verify the proposed protocol with the Soft-EdgeNet model [37] and MADIT [39] with a different number of sensors and malicious nodes. The simulation environment is comprised of sensors, mobile agents, and a sink node. They are distributed at random over a 200 × 200 m area. The transmission range of each sensor is set at 5 m. Nodes have heterogeneous initial energies between 2j and 5j. We assume five mobile agents and two sink nodes. Agents are considered edge devices and collaborate with both the sensor nodes and the mobile sink. The communication link is assumed to be asymmetric, and the packet size is set to 32 bytes. The number of sensors varies between 20 and 100. Table 2 shows the simulation parameters. The performance metrics of energy consumption, end-to-end delay, computing overheads, and detection rate as discussed in [41,42] are evaluated for the proposed protocol and related studies.

Table 2. Default simulation parameters.

Parameter	Value
Nodes	20–100
Sink nodes	2
Field dimension	200 m × 200 m
Initial energy	2–5j
Transmission range	5 m
Packet size	32 bytes
Time intervals	2000 s
Number of simulations	10
Mobile agents	5
Malicious devices	2–10

4.1. Security Analysis of Proposed Protocol

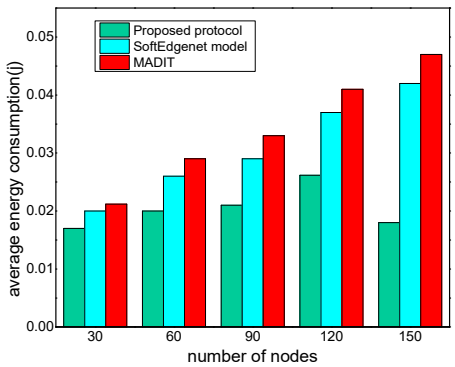
In this section, we list numerous network risks along with the developed countermeasures. Table 3 illustrates the developed procedures for the assurance of security analysis.

Table 3. Security analysis.

Attack	Proposed Countermeasures
Replay attack	Time stamp, pseudorandom
Token security	Encrypted with a session key
Data privacy	Xor between data blocks and new session key
Mutual trust	Exchange of security tokens
Non-verifiable trust	System authentication error
Security for session key	Encryption layer using public key
Route failure	Resend security token
Data modification	Digital hash
Erroneous data packets	Timely detection of faulty nodes/links

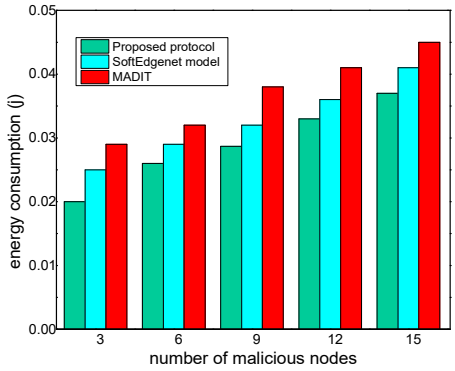
4.2. Results

We compared the efficiency of the proposed protocol with other solutions for energy consumption. It is defined as the usage of energy resources of the nodes in the sensing, aggregation, and transmission of data packets. Figure 3a,b shows the comparison of the proposed protocol with existing solutions, and it reveals that the proposed protocol has an improvement of 13% and 15% in terms of energy efficiency. The proposed protocol smoothly chooses the updated routes while providing a robust decision based on a fitness function. Moreover, by investigating multiple parameters, the position of cluster heads is rotated. Furthermore, due to the early detection of faulty links, the proposed solution decreases the data loss rate and ultimately offers the lowest number of control messages and retransmissions. As a result, it efficiently utilizes the energy consumption of nodes. Moreover, the agent tables are only adjusted when any reasonable changes occur around the proximity of agents.



(**a**)

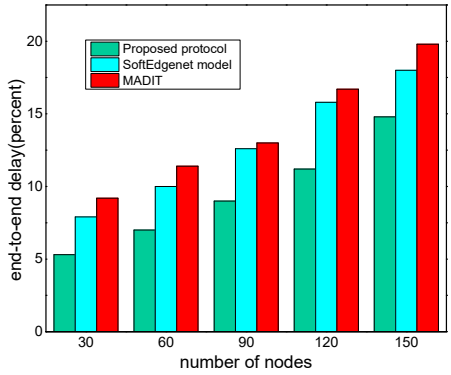
Figure 3. *Cont.*



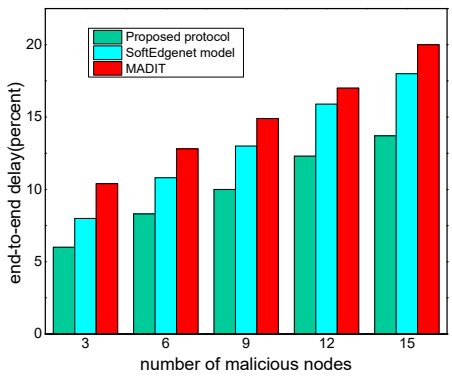
(**b**)

Figure 3. (**a**) Energy consumption and sensor nodes; (**b**) energy consumption and malicious nodes.

Figure 4a,b compares the proposed protocol and other studies in terms of the end-to-end delay. It can be described as the amount of time it takes a packet to transit across a network from the source to the destination. According to the findings, the proposed protocol, when compared to alternative studies, minimizes the end-to-end latency by 15% and 18%, respectively. This is because mobile agents are integrated across the specified clusters' boundaries, and the role of cluster heads is rotated by investigating the fitness functions. Furthermore, based on the preset threshold, the probability of nodes also increases for the selection of cluster heads. The mobile agents balance the traffic overhead on the connected nodes, as well as shorten the time it takes to acquire IoT data.



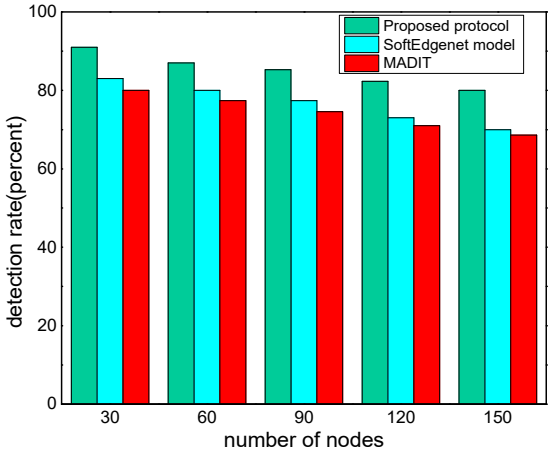
(**a**)



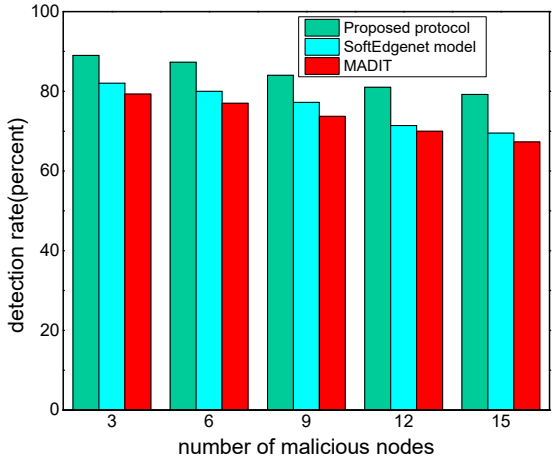
(**b**)

Figure 4. (**a**) End-to-end delay and sensor nodes; (**b**) end-to-end delay and malicious nodes.

Figure 5a,b shows the detection rate results for the proposed protocol and other existing work under varying numbers of normal and malicious devices. It is described as a ratio of the number of precisely analyzed faulty packets to the total number of transmitted packets. It was seen that the proposed protocol significantly reduces malicious traffic by 15% and 18% in the existence of unreliable devices. This is due to the generation of security tokens and devices are mutually authenticated using random numbers. Furthermore, the secret keys and random numbers help the IoT system's data to be available quickly and allow the rapid detection of malicious devices. The mobile agents are also more reliable and serve as a supervisor for IoT data without overloading the cluster heads. Later, the collected data are sent to the application user with the system's intelligence decision.



(**a**)

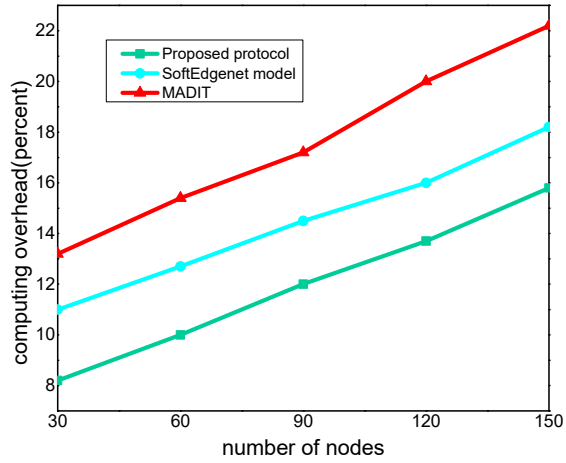


(**b**)

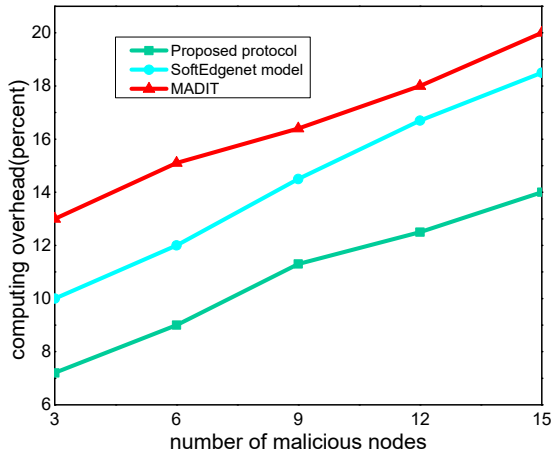
Figure 5. (**a**) Detection rate and sensor nodes; (**b**) detection rate and malicious nodes.

Figure 6a,b shows the performance results of the proposed protocol and the existing solution in terms of computing overheads. It is defined as the sending of control packets from a source node to a destination for the accomplishment of data routing. The proposed protocol reduces communication costs by 14% and 17%, respectively, while using different normal and malicious devices. This is due to the proposed protocol exploiting the mobile agents and optimizing the route-learning process with the distribution of balanced power consumption. The mobile agent migrates around the clusters and obtains the data from the respective cluster head. Moreover, the objective function is based on the measurement of the distance, energy, and error level, which helps to identify the forwarders and reduce the

number of dropped packets. The number of retransmissions is thereby minimized by the proposed protocol, which also decreases additional communication costs. Additionally, the proposed protocol recomputes the suitability of the nodes and assigns a probability when the cost value is below a specific level.



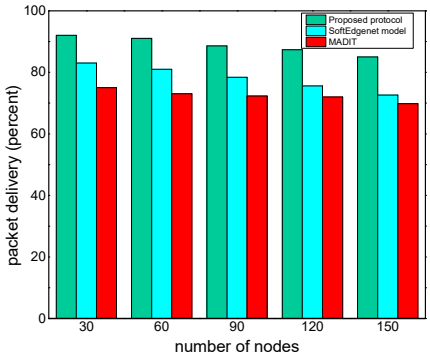
(**a**)



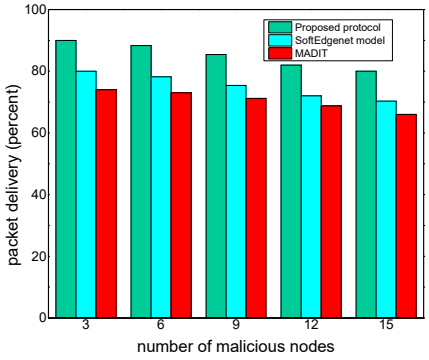
(**b**)

Figure 6. (**a**) Computing overheads and sensor nodes; (**b**) computing overheads and malicious nodes.

The proposed protocol is evaluated in terms of the packet delivery ratio against existing work. It is defined as the number of successfully received packets to the total number of transmitted packets. Figure 7a,b depict its performance and simulation-based results, which demonstrate the improved efficacy of the proposed protocol by 15% and 17%, respectively. This is due to the exploration of mobile agents that migrate among cluster heads and reduce the additional energy consumption for IoT systems. Furthermore, the weighted cost for the best routes chosen for data forwarding increases the lifetime of the network while decreasing the error rate over the links. The proposed security procedures also offer trust among mobile agents and IoT nodes, and as a result, increase the delivery performance of the deployed network with sink nodes.



(**a**)



(**b**)

Figure 7. (**a**) Packet delivery and sensor nodes; (**b**) packet delivery and malicious nodes.

5. Conclusions

This paper describes a mobile agent-based edge protocol for providing energy-efficient systems while maintaining mutual trust and security. The proposed protocol ensures consistent transmission over insecure channels and creates intelligent computing for network distribution. It also optimizes traffic flow on edge devices through the integration of mobile agents that move around the cluster heads and obtain data while reducing energy consumption in a balanced manner. Furthermore, mutual trust is established between mobile agents and sensor nodes for transferring IoT data, and end-users are authorized to obtain the requested information following the verification of connected devices. However, it has been noted that when a large number of devices are rapidly changing positions, the proposed protocol imposes a link failure and is unable to control network congestion at edge locations. Therefore, we aim to implement a machine-learning technique in the system to improve the quality of services between constraint devices and efficiently handle the distributed communication threats.

Author Contributions: Conceptualization, M.E. and K.H.; methodology, M.E.; software, M.N.; validation, M.S., M.A. and M.I.A.; formal analysis, M.I.A. and M.N.; investigation, M.E.; resources, M.N.; data curation, K.H.; writing—original draft preparation, M.E.; writing—review and editing, K.H.; visualization, M.S.; supervision, M.S.; project administration, M.E.; funding acquisition, M.E. and M.I.A. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: All data are available in the manuscript.

Acknowledgments: All authors are thankful for their technical support.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Islam, N.; Altamimi, M.; Haseeb, K.; Siraj, M. Secure and Sustainable Predictive Framework for IoT-Based Multimedia Services Using Machine Learning. *Sustainability* **2021**, *13*, 13128. [CrossRef]
2. Dai, H.-N.; Zheng, Z.; Zhang, Y. Blockchain for Internet of Things: A survey. *IEEE Internet Things J.* **2019**, *6*, 8076–8094. [CrossRef]
3. Hassan, W.H. Current research on Internet of Things (IoT) security: A survey. *Comput. Netw.* **2019**, *148*, 283–294.
4. Fortino, G.; Messina, F.; Rosaci, D.; Sarne, G.M.L. Using blockchain in a reputation-based model for grouping agents in the Internet of Things. *IEEE Trans. Eng. Manag.* **2019**, *67*, 1231–1243. [CrossRef]
5. Qadori, H.Q.; Zukarnain, Z.A.; Hanapi, Z.M.; Subramaniam, S. FuMAM: Fuzzy-based mobile agent migration approach for data gathering in wireless sensor networks. *IEEE Access* **2018**, *6*, 15643–15652. [CrossRef]
6. Kumar, S.; Chaurasiya, V.K. A strategy for elimination of data redundancy in internet of things (IoT) based wireless sensor network (wsn). *IEEE Syst. J.* **2018**, *13*, 1650–1657. [CrossRef]
7. Ullah, A.; Said, G.; Sher, M.; Ning, H. Fog-assisted secure healthcare data aggregation scheme in IoT-enabled WSN. *Peer-Peer Netw. Appl.* **2020**, *13*, 163–174. [CrossRef]
8. Rehman, A.; Haseeb, K.; Saba, T.; Lloret, J.; Tariq, U. Secured Big Data Analytics for Decision-Oriented Medical System Using Internet of Things. *Electronics* **2021**, *10*, 1273. [CrossRef]
9. Malik, H.; Zatar, W. Agent based routing approach to support structural health monitoring-informed, intelligent transportation system. *J. Ambient. Intell. Humaniz. Comput.* **2020**, *11*, 1031–1043. [CrossRef]
10. Venetis, I.E.; Gavalas, D.; Pantziou, G.E.; Konstantopoulos, C. Mobile agents-based data aggregation in WSNs: Benchmarking itinerary planning approaches. *Wirel. Netw.* **2018**, *24*, 2111–2132. [CrossRef]
11. Dai, H.-N.; Wong, R.C.-W.; Wang, H.; Zheng, Z.; Vasilakos, A.V. Big data analytics for large-scale wireless networks: Challenges and opportunities. *ACM Comput. Surv.* **2019**, *52*, 1–36. [CrossRef]
12. Yue, Y.-G.; He, P. A comprehensive survey on the reliability of mobile wireless sensor networks: Taxonomy, challenges, and future directions. *Inf. Fusion* **2018**, *44*, 188–204. [CrossRef]
13. Dehkordi, S.A.; Farajzadeh, K.; Rezazadeh, J.; Farahbakhsh, R.; Sandrasegaran, K.; Dehkordi, M.A. Survey on data aggregation techniques in IoT sensor networks. *Wirel. Netw.* **2020**, *26*, 1243–1263. [CrossRef]
14. Verma, S.; Gain, S. Mitigating hot spot problem in wireless sensor networks using political optimizer based unequal clustering technique. *J. Cybersecur. Inf. Manag.* **2021**, *8*, 42–50. [CrossRef]
15. Younan, M.; Khattab, S.; Bahgat, R. From the wireless sensor networks (WSNs) to the Web of Things (WoT): An overview. J. Intell. Syst. *Int. Things* **2021**, *4*, 56–68.
16. Chen, B.; Bai, R.; Li, J.; Liu, Y.; Xue, N.; Ren, J. A multiobjective single bus corridor scheduling using machine learning-based predictive models. *Int. J. Prod. Res.* **2020**, 1–16. [CrossRef]
17. Ahmed, I.; Ahmad, M.; Rodrigues, J.J.P.C.; Jeon, G. Edge computing-based person detection system for top view surveillance: Using CenterNet with transfer learning. *Appl. Soft Comput.* **2021**, *107*, 107489. [CrossRef]
18. Qin, W.; Zhuang, Z.; Huang, H. A novel reinforcement learning-based hyper-heuristic for heterogeneous vehicle routing problem. *Comput. Ind. Eng.* **2021**, *156*, 107252. [CrossRef]
19. Singh, S.P.; Nayyar, A.; Kumar, R.; Sharma, A. Fog computing: From architecture to edge computing and big data processing. *J. Supercomput.* **2019**, *75*, 2070–2105. [CrossRef]
20. Rani, R.; Kumar, N.; Khurana, M.; Kumar, A.; Barnawi, A. Storage as a service in Fog computing: A systematic review. *J. Syst. Archit.* **2021**, *116*, 102033. [CrossRef]
21. Li, B.; He, M.; Wu, W.; Sangaiah, A.K.; Jeon, G. Computation offloading algorithm for arbitrarily divisible applications in mobile edge computing environments: An OCR case. *Sustainability* **2018**, *10*, 1611. [CrossRef]
22. Din, S.; Ahmad, A.; Paul, A.; Jeon, G. *Software-Defined Internet of Things to Analyze Big Data in Smart Cities, in Edge Computing*; Springer: Cham, Switzerland, 2019; pp. 91–106. [CrossRef]
23. Khan, M.; Iqbal, J.; Talha, M.; Arshad, M.; Diyan, M.; Han, K. Big data processing using internet of software defined things in smart cities. *Int. J. Parallel Progr.* **2020**, *48*, 178–191. [CrossRef]
24. Shankar, K. Improving the security and authentication of the cloud with iot using hybrid optimization based quantum hash function. *J. Intell. Syst. Internet Things* **2021**, *1*, 61–71. [CrossRef]
25. Kumar, D.P.; Amgoth, T.; Annavarapu, C.S.R. Machine learning algorithms for wireless sensor networks: A survey. *Inf. Fusion* **2019**, *49*, 1–25. [CrossRef]
26. Zhao, B.; Liu, J.; Wei, Z.; You, I. A deep reinforcement learning based approach for energy-efficient channel allocation in satellite internet of things. *IEEE Access* **2020**, *8*, 62197–62206. [CrossRef]
27. Ahmed, I.; Jeon, G.; Piccialli, F. A deep-learning-based smart healthcare system for patient's discomfort detection at the edge of Internet of Things. *IEEE Int. Things J.* **2021**, *8*, 10318–10326. [CrossRef]
28. Khan, L.U.; Yaqoob, I.; Tran, N.H.; Kazmi, S.A.; Dang, T.N.; Hong, C.S. Edge computing enabled smart cities: A comprehensive survey. *IEEE Int. Things J.* **2020**, *7*, 10200–10232. [CrossRef]
29. Sun, X.; Ansari, N. EdgeIoT: Mobile edge computing for the Internet of Things. *IEEE Commun. Mag.* **2016**, *54*, 22–29. [CrossRef]
30. Dong, Y.; Guo, S.; Liu, J.; Yang, Y. Energy-efficient fair cooperation fog computing in mobile edge networks for smart city. *IEEE Int. Things J.* **2019**, *6*, 7543–7554. [CrossRef]

31. Huang, J.; Li, S.; Chen, Y. Revenue-optimal task scheduling and resource management for IoT batch jobs in mobile edge computing. *Peer-Peer Netw. Appl.* **2020**, *13*, 1776–1787. [CrossRef]
32. Marques, P.; Manfroi, D.; Deitos, E.; Cegoni, J.; Castilhos, R.; Rochol, J.; Pignaton, E.; Kunst, R. An IoT-based smart cities infrastructure architecture applied to a waste management scenario. *Ad. Hoc. Netw.* **2019**, *87*, 200–208. [CrossRef]
33. Pourghebleh, B.; Wakil, K.; Navimipour, N.J. A comprehensive study on the trust management techniques in the Internet of Things. *IEEE Internet Things J.* **2019**, *6*, 9326–9337. [CrossRef]
34. El Fissaoui, M.; Beni-Hssane, A.; Saadi, M. Multi-mobile agent itinerary planning-based energy and fault aware data aggregation in wireless sensor networks. *EURASIP J. Wirel. Commun. Netw.* **2018**, *2018*, 1–11. [CrossRef]
35. Sellami, B.; Hakiri, A.; Ben Yahia, S.; Berthou, P. Energy-aware task scheduling and offloading using deep reinforcement learning in SDN-enabled IoT network. *Comput. Netw.* **2022**, *210*, 108957. [CrossRef]
36. Savaglio, C.; Pace, P.; Aloi, G.; Liotta, A.; Fortino, G. Lightweight reinforcement learning for energy efficient communications in wireless sensor networks. *IEEE Access* **2019**, *7*, 29355–29364. [CrossRef]
37. Sharma, P.K.; Rathore, S.; Jeong, Y.-S.; Park, J.H. SoftEdgeNet: SDN based energy-efficient distributed network architecture for edge computing. *IEEE Commun. Mag.* **2018**, *56*, 104–111. [CrossRef]
38. Zhang, W.; Liu, Y.; Han, G.; Feng, Y.; Zhao, Y. An energy efficient and QoS aware routing algorithm based on data classification for industrial wireless sensor networks. *IEEE Access* **2018**, *6*, 46495–46504. [CrossRef]
39. Alsboui, T.; Qin, Y.; Hill, R.; Al-Aqrabi, H. Enabling distributed intelligence for the Internet of Things with IOTA and mobile agents. *Computing* **2020**, *102*, 1345–1363. [CrossRef]
40. Yousefi, S.; Derakhshan, F.; Karimipour, H.; Aghdasi, H.S. An efficient route planning model for mobile agents on the internet of things using Markov decision process. *Ad. Hoc. Netw.* **2020**, *98*, 102053. [CrossRef]
41. Sennan, S.; Balasubramaniyam, S.; Luhach, A.K.; Ramasubbareddy, S.; Chilamkurti, N.; Nam, Y. Energy and delay aware data aggregation in routing protocol for Internet of Things. *Sensors* **2019**, *19*, 5486. [CrossRef]
42. Masdari, M.; Özdemir, S. Towards coverage-aware fuzzy logic-based faulty node detection in heterogeneous wireless sensor networks. *Wirel. Pers. Commun.* **2020**, *111*, 581–610. [CrossRef]