A Mobility Management Algorithm in the Internet of Things (IoT) for Smart Objects based on Software-Defined Networking (SDN)

Lili Pei
Department of Architectural Engineering
Tangshan Polytechnic College
Tangshan, 063299, China

***Abstract*—In recent decades, technological advancements have significantly improved people's living standards and given rise to the rapid development of intelligent technologies. The Internet of Things (IoT) is one of the most important research topics worldwide. However, IoT is often comprised of unreliable wireless networks, with hundreds of mobile sensors interconnected. A traditional sensor network typically consists of fixed sensor nodes periodically transmitting data to a pre-determined router. Current applications, however, require sensing devices to be mobile between networks. We need mobility management protocols to manage these mobile nodes to provide uninterrupted service to users. The interactions between the mobile nodes are affected by the loss of signaling messages, increased latency, signaling costs, and energy consumption because of the characteristics of these networks, including constrained memory, processing power, and limited energy source. Hence, developing an algorithm for managing smart devices' mobility on the Internet is necessary. This study proposes an efficient and effective distributed mechanism to manage mobility in IoT devices. Using Software-Defined Networking (SDN) based on the CoAP protocol, the proposed method is intended not only to reduce the signaling cost of messages but also to make mobility management more reliable and simpler.**

Keywords—Internet of things (IoT); mobility management; software-defined networking (SDN); CoAP protocol

I. Introduction

In recent years, Internet of Things (IoT) technology has been used in multiple areas, including health supervision, crisis management, and transportation management. IoT is an information network of physical objects (sensors, machines, devices, etc.) that facilitates communication and cooperation between these objects to reach a specific aim [1-3]. Each device within the IoT can identify, evaluate, and interact with the existing internet infrastructure using its embedded system. In other words, the IoT is a computational concept that can describe a future in which physical objects are connected using the internet and create a network of connections with other objects. In this technology, each entity on the internet is assigned a Unique Identifier (UI) and an Internet Protocol (IP) address through which it can send the data to the designated databases [4-6].

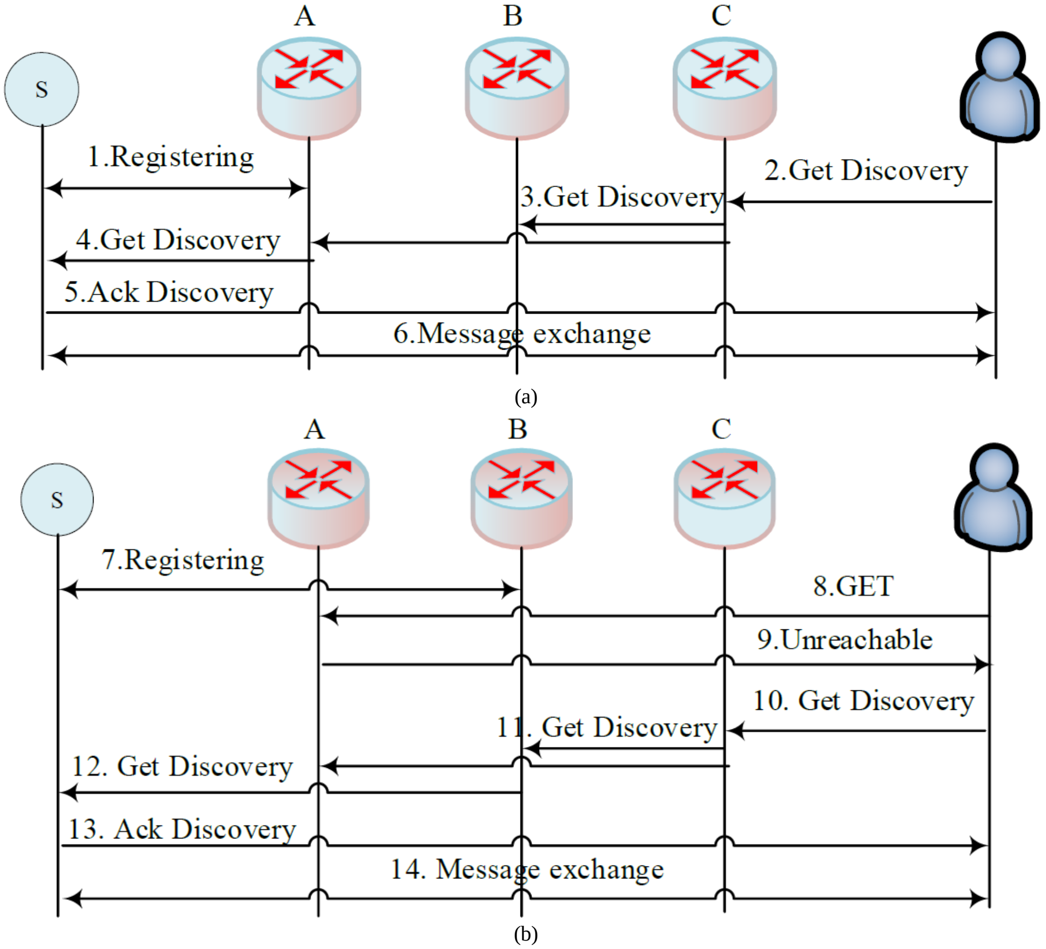
The Internet Engineering Task Force (IETF) has introduced various standards for the interactions between web services and a network of smart objects. For instance, Constrained Application Protocol (CoAP) is an application layer protocol modeled based on the Representational State Transfer (REST) software architectural style that facilitates the communication between the resource-constrained devices and web services within the IoT infrastructure. CoAP is a simple and modified version of the Hypertext Transfer Protocol (HTTP) designed in 2013. In CoAP, two messages are mainly used: Confirmable (CON) to signal secure connections and Non-Confirmable (NON) to signal regular connections. When receiving the CON message, the receiver sends an acknowledgment message to indicate that the message was received correctly. If the acknowledgment message is not received, the CON message is sent out again after a specific time. Therefore, this format provides the ability to resend messages which, in turn, creates an atmosphere of trust within the entire network. Fig. 1 demonstrates the CoAP retransmission mechanism. Chun et al. [7] introduced an algorithm for retransmission management based on the CoAP retransmission mechanism that incorporates the features and message formats of CoAP.

Software-Defined Networking (SDN) has three layers: the infrastructure layer (data plane), the control layer (control plane), and the application layer [8]. The infrastructure layer, also known as the data plane, consists of the packet delivery elements (routers and switches). The control layer is the logical architecture of the software that sets out the delivery codes for the elements within the infrastructure layer while managing the networking and routing tasks. Separating the data and control planes enables the network operator to control the network behavior from the top down. The application layer manages the applications within the network. Software-Defined Networking (SDN) introduces the technology of a centralized network controller that increases network scalability and flexibility by separating the control and data planes. Zhou and Zhang [9] introduce a host-based method that uses SDN technology to improve mobile IP and manage filtering and routing. The problem with this method is that it requires a hostname and IP address change. Furthermore, Raza et al. [10] introduced a network-based retransmission method that sets out an OpenFlow-based Proxy Mobile IPv6 (PMIPv6) protocol. This method separates the signaling control route from the communication data path. However, using Mobile Nodes (MN) to send Router Solicitation (RS) messages and using the network to send Router Advertisement (RA) messages leads to significant delays within the system. Furthermore, this method uses an IP tunnel instead of an OpenFlow, which requires more network overhead. Chen et al. [11] introduced an SDN-based retransmission protocol that decreases the retransmission timeout. In this method, network switches occur in parallel and simultaneously with layer two switches. At the same time, active currents are delivered to all possible target channels. Network switch configuration takes place through an optimal track method.

Unfortunately, most IP-based standard Transmission Control Protocols (TCPs) are incompatible with IoT infrastructure [12, 13]. IoT structure consists of hundreds of interconnected mobile sensor nodes. Since these sensors have constrained memory, processing ability, computing ability, and energy resources, they introduce multiple challenges to the system that can impact delay-sensitive applications. On the other hand, most standard TCPs, such as Mobile IPv6 (MIPv6), have significant signaling overhead for tunneling and binding. That is why they impose a significant processing overhead on the network [14, 15]. Within the IoT ecosystem, mobile sensor nodes should be able to deliver the analyzed data to the remote user periodically. As a result, IoT requires a new protocol to control transmission that can meet the various needs of the system based on mobile sensors' features while operating on a constrained energy and sleep mode. In this study, to come up with a solution for this problem, instead of using IP-based standard TCPs, CoAP and SDN-based TCPs are used since they introduce an effective transmission control mechanism for mobile sensor nodes while decreasing signaling costs.

To get a clear overview of the research, short descriptions of the structure of the research paper are summarized as follows:

- Section II: In this section, the details of the proposed solution for managing the mobile nodes of the resource-constrained in the IoT will be examined.
- Section III: This section will evaluate and compare the proposed solution with previous methods in this field.
- Section IV: In this section, the summary and conclusion of the results will be presented.



(a)

(b)

Fig. 1. CoAP Retransmission Mechanism: (a) Before Retransmission, (b) After Retransmission.

II. Proposed SDN-based Transmission Control Algorithm

A. *Intra-Domain and Inter-Domain Transmission*

Fig. 3 demonstrates what transpired before and after the Intra-Domain transmission. The order of the exchanged messages and their related reactions are included in the following:

- Phase 1: Mobile Node (MN) service network delivers the “weak signal” message to the controller.
- Phase 2: After receiving the “weak signal” message, the controller examines the transmission protocol of all neighboring networks to identify the host channels. Then, all the active currents receive the mobile nodes from the current manager and compute the number of routes needed for multicasting.
- Phase 3: After computing the routes, the manager delivers the current change messages to adjust routing tables in the associated networks.
- Phase 4: CoAP-based Mobile Node, while entering a domain, by exchanging the Power-On Self-Test (POST) message, records its IP address within the network and receives an acknowledgment message.
- Phase 5: The network informs the controller of a new mobile sensor connection and sends the mobile sensor’s IP address within the report to the controller.
- Phase 6: After receiving the network’s message, the controller sends the current change messages to the host networks to eliminate the unnecessary currents.

Fig. 4 demonstrates the order of the exchanged messages in inter-domain transmissions. As demonstrated in Fig. 4, Phases 1, 2, and 3 in this method are similar to intra-domain transmission. The source controller sends out the pre-transmission request to the location server. The location server identifies host networks and sends requests to their domain controllers. When the host network’s controller receives the request, it estimates the pre-transmission route and sets out the current tables. In the final phase, by delivering the address report, the target network informs the controller of a new node connection within its domain. The controller transmits the update message to the location server. The location server updates the new location of the mobile sensor node. It sends out the transmission report to Primary Site Controller (PSC). After receiving the report, the controller eliminates the information related to the transmitted mobile node and the extra currents. Fig. 2 shows the SDN controller architecture in the IoT.

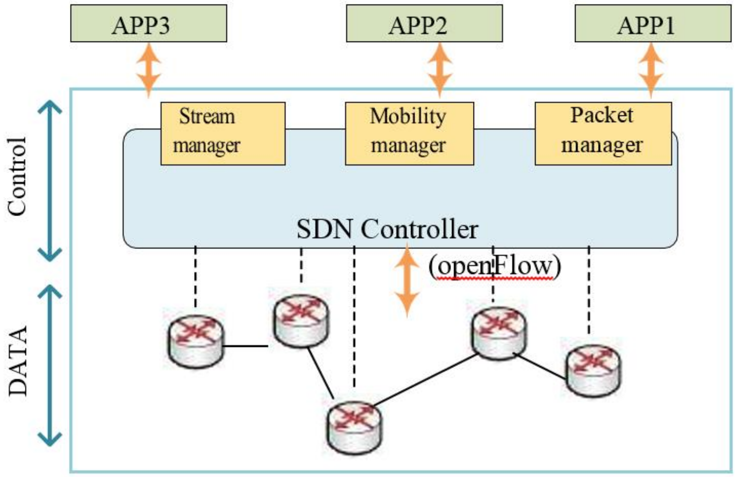


Fig. 2. SDN Controller Architecture in the IoT.

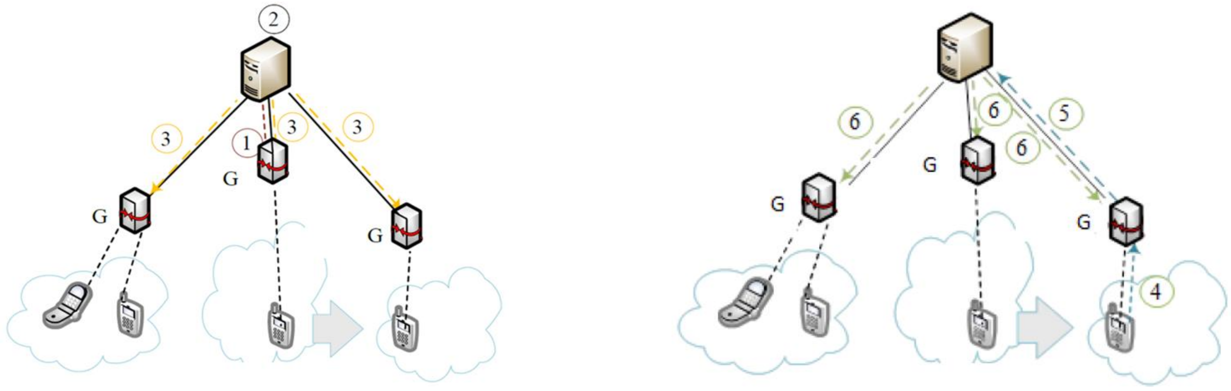
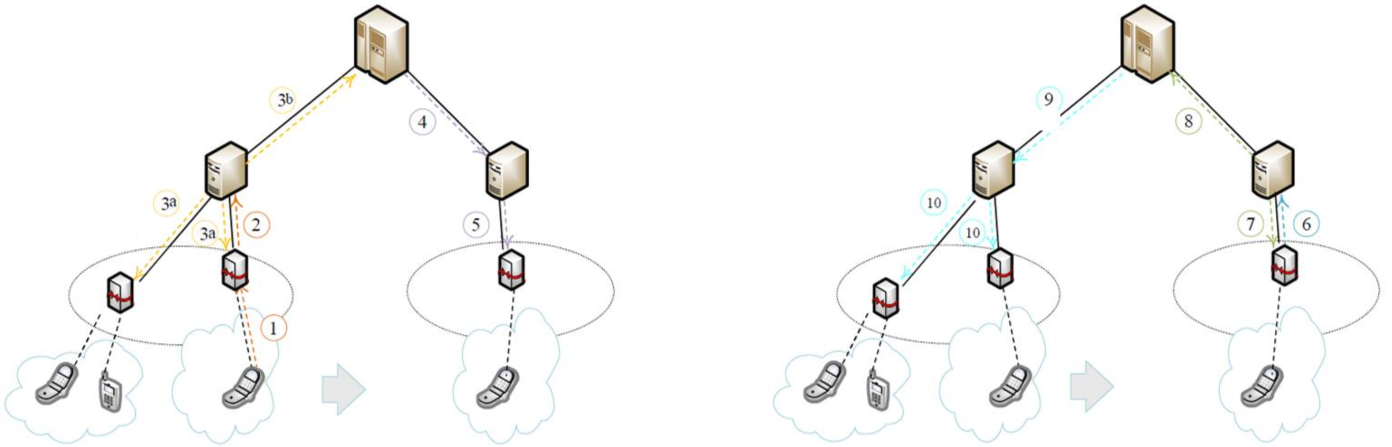


Fig. 3. Intra-Domain Transmission: a) Intra-Domain Pre-Transmission, b) Completed Intra-Domain Transmission.



a) b)

Fig. 4. Inter-Domain Transmission: a) Inter-Domain Pre-Transmission, b) Completed Inter-Domain Transmission.

B. Transmission Delay and Signaling Costs Analysis

CoAP provides End-to-End Security using CON messages and a Stop-and-Wait Automatic Repeat Request (ARQ) mechanism. If the mobile node does not receive an ACK for its CoAP Confirmable Message (CON) within a specific time, it retransmits the same CON.

Based on the calculations done in [7], the packet loss ratio in the wireless transmission is calculated through the following equation:

$$P = 1 - (1 - S)^{2m} \tag{1}$$

In which *S* is the sampling error and *m* is the packet length.

The Packet Error Rate (PER) in the application layer is calculated through the following equation:

$$E = P^{c+1} \tag{2}$$

In which *c* equates to the maximum number of retransmissions in the MAC layer.

When it comes to packet segmentation in CoAP, Packet Error Rate is calculated by:

$$E_s = \sum_{i=1}^{s} E \times (1 - P)^{i-1} \tag{3}$$

The maximum number of packages is 12.

The probability of message delivery for *i* times of P_R retransmission of a CoAP message using the *s* packet is estimated through the following formula:

$$P_R^i = (1 - E_s) \times E_s^i \tag{4}$$

Therefore, the average retransmission time for each CoAP message is:

$$E\,(R) = \sum_{i=0}^{m-1} i \times P_R^i + (m - 1) \times E_s^m \tag{5}$$

in which *m* is the maximum count of message retransmission that the internet-connected system can approve.

If m is the maximum number of message retransmission, then the probability of a CoAP message not being delivered is E_s^{m+1} and the probability of its successful transmission is $\tau = 1 - E_s^{m+1}$. Since *n* sensors are competing with each other to transmit the messages within the channel, the probability of having at least one successful transmission in each time slot is:

$$P_s = 1 - (1 - \tau)^n \tag{6}$$

Therefore, the possibility of successful transmission within a channel provided that only one sensor transmits the message is calculated by the following formula:

$$P_{succ} = \frac{n\tau\,(1-\tau)^{n-1}}{1-(1-\tau)^n} \tag{7}$$

At this point, while taking into account Round Trip Time (RTT) and the time required for receiving the Acknowledgment report for each message (T_{ACK}), we calculated the delayed signaling messages in CoAP, which is estimated at:

$$D = \sum_{i=0}^{m-1} P_R^i \times (RTT + T_{ACK}) + E_s^m \times T_{ACK} \tag{8}$$

RTT is the time from the point of message transmission to the point of receiving a response estimated through the following equation:

$$RTT = \alpha \times old\ RTT + (1 - \alpha) \times new\ RTT \tag{9}$$

In this equation, α is always between 0 and 1.

Finally, the signaling costs can be estimated from the following formula while taking into account the Packet Length (*Lp*) and Packet Arrival Rate:

$$C_p = \lambda_s \times L_p \times D \tag{10}$$

In which λ_s is the packet arrival rate, *Lp* is the Packet Length, and *D* is the packet transmission delay.

III. Results and Data Analysis

In this study, we used the two methods of mathematical simulation and analysis to examine the effectiveness of the proposed algorithm. In the simulation method, the study is based on the grounds that it matches the circumstances in real-life situations and operational networks as much as possible. There are various simulators, including OMNet++, NS, and Opnet. Opnet is one of the most powerful and popular simulators that many researchers use to simulate their proposed models. To examine the effectiveness of the proposed algorithm, we implemented it in the Opnet simulator to compare it with the algorithm introduced by Chun et al. [7]. We used Matlab software to analyze the derived mathematical models.

A. Evaluation Criteria

The proposed algorithm should be assessed based on the basic algorithm to examine its performance of the proposed algorithm. To examine algorithm efficiency, some parameters should be studied that are included in the following:

- Signaling Latency: the time it takes for a signaling message to be transmitted and received indicates the signaling Latency.
- End-to-End Delay: the time it takes to send a request and receive its response is the end-to-end Delay. End-to-End Delay consists of signaling time, request transmission time within the link, and the time required to receive the Acknowledgment message and its response.
- Traffic Load: this parameter indicates the number of packets transmitted within the network at any time.
- Throughput: the average data packet successfully transmitted within the network is called network throughput. Network throughput is typically measured in bits per second or packets per second. In this study, the packet's network throughput is measured per second.
- Signaling Cost: The average costs of the exchanged signaling messages are measured based on the packet length and link latency.

Successful Transmission Probability Rate: successful transmission probability rate is measured by dividing the number of packets that were transmitted successfully within the channels by the total number of packets.

B. Results of the Proposed Algorithm Analysis

Within the IoT ecosystem, retransmission delay and the packet loss ratio are two of the most significant factors in evaluating the transmission algorithm. Channel delay and error rates are calculated by the formula introduced in the previous section. In this part of the study, we implemented Matlab's resulting correlations and calculated the transmission delay and signaling costs. To examine the system's efficiency, we provided networks of sensors that have n mobile sensors connected to the internet using a network. Networks support the OpenFlow protocol through which they connect to the controller.

On the other hand, the networks are connected to the sensor nodes using CON messages in CoAP. The parameters used in this analysis are similar to the ones used by Makaya and Pierre [16] in Table I. The bandwidth of the wireless network and the wired network are 250 kilobits per second and 10 megabits per second, respectively.

TABLE I. THE PARAMETERS USED IN THIS STUDY

Parameter	**Value**
Wireless link latency	15 ms
Wired link latency	2 ms
Wired bandwidth	10 Mbps
Wireless bandwidth	250 kbps
Average node speed	10 m/s

Fig. 5 demonstrates how RTT affects signaling message latency. As demonstrated in Fig. 5, transmission delay increases signaling latency. However, the Quality of Service (QoS) requirements' impact on signaling latency depends on the internet packet types (IP packet or CoAP packet) and the number of parts within each packet. Fig. 5 demonstrates that small network packets impose fewer network delays than the packets that contain more parts. This parameter begins to increase in network packets that have more parts. That is to say, for more extensive data packets, latency occurs mainly because of the traffic competition in the channel and not because of the multitude of packet parts.

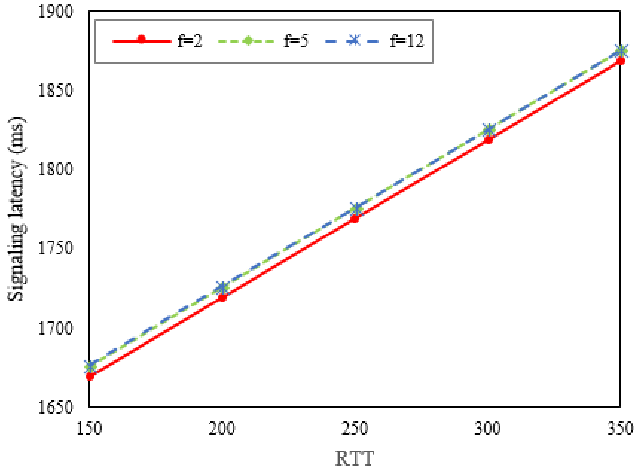


Fig. 5. Signaling Latency Caused by Round Trip Time (RTT) Variations.

Fig. 6 demonstrates signaling costs based on the variation in entry rates. As demonstrated in Fig. 6, when entry rates increase, signaling costs increase, as well. The competition between the nodes for packet transmission within the channel increases the number of packet retransmissions within the channel, which, in turn, raises signaling costs.

The probability of successful transmission based on the number of sensor nodes within the network is demonstrated in Fig. 7. As demonstrated in Fig. 7, the successful transmission rate decreases with increased sensors within the network. This parameter can positively impact the retransmission rate and signaling costs.

C. *Proposed Algorithm Simulation*

In this study section, we introduce the structure of the simulation modeling of the M-CoSDN transmission mechanisms. An Opnet simulator was employed in this study for simulation modeling. Furthermore, this study provides a comparative analysis of the M-CoSDN proposed algorithm and the algorithm proposed by Chun et al. [7].

Fig. 8 demonstrates the network topology of the inter-domain simulation mainly used in transmission management studies. A 200 × 200 Wireless Sensor Network (WSN) with a range of 50 meters was chosen for this study. Each trajectory covers around 20 meters. A specific packet is introduced for each exchanged message during the signaling process. A specific packet based on the protocol format was introduced for the controller's response, acknowledgment, and current messages. In this study, the average incoming request time is not changed and is calculated every two milliseconds. Therefore, the incoming requests are transmitted to the controller every two milliseconds.

Fig. 9 demonstrates the End-to-End Delay within M-CoSDN proposed algorithm and the basic algorithm. As predicted, End-to-End Delay within the proposed algorithm is much lower than the basic algorithm. Using a central controller for transmission control that transmits current messages and controls the network’s topology and sensors accelerates transmission. That is why the proposed algorithm detects a few delays.

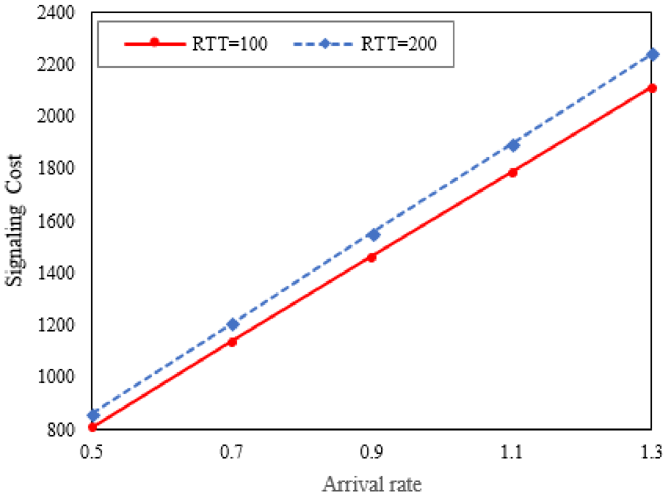


Fig. 6. Signaling Costs Caused by Increasing Entry Rates.

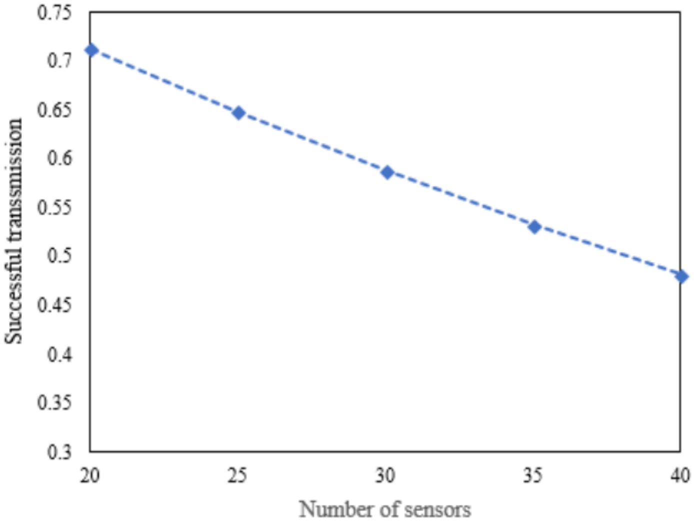


Fig. 7. Successful Transmission Probability within the Channel is Caused by Variance in the Number of Sensor Nodes.

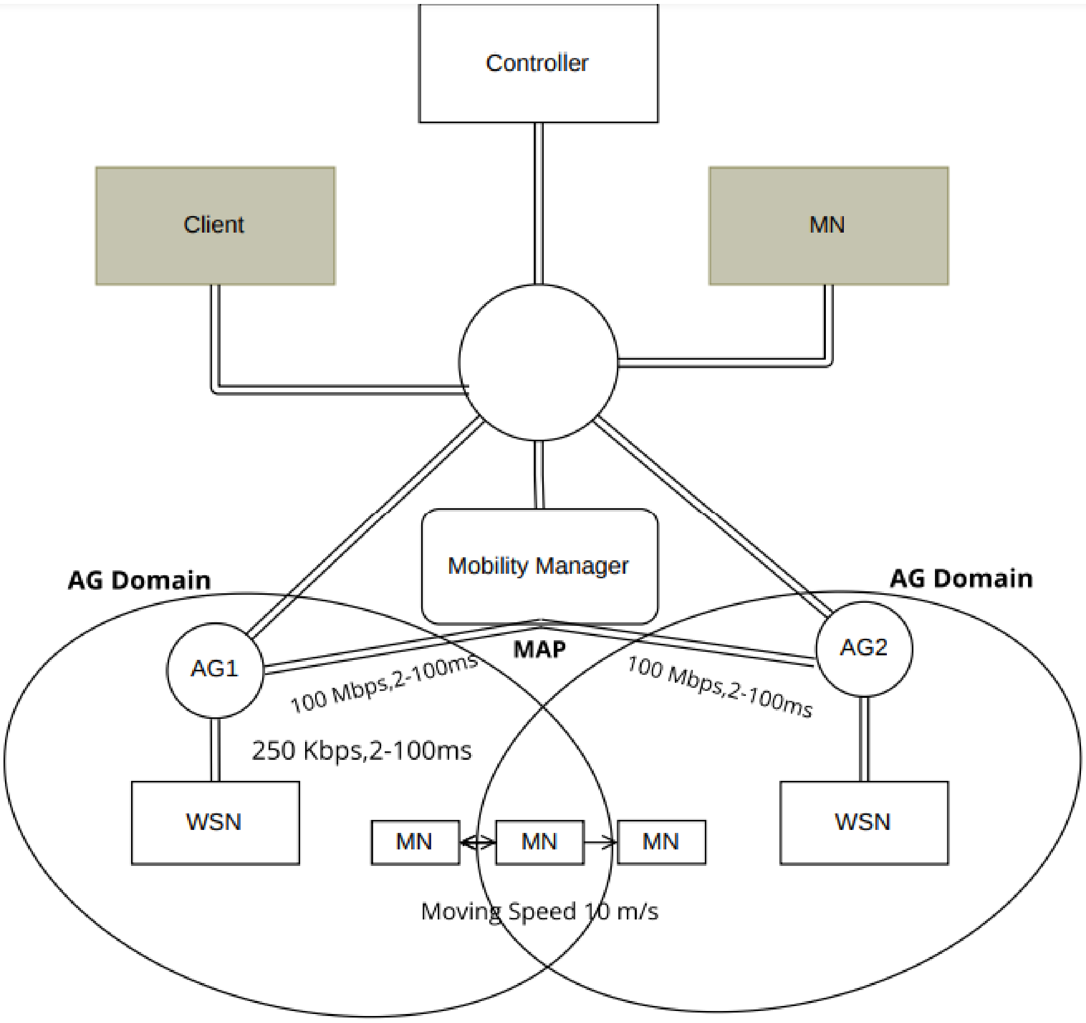


Fig. 8. Network Topology and Simulation Parameters.

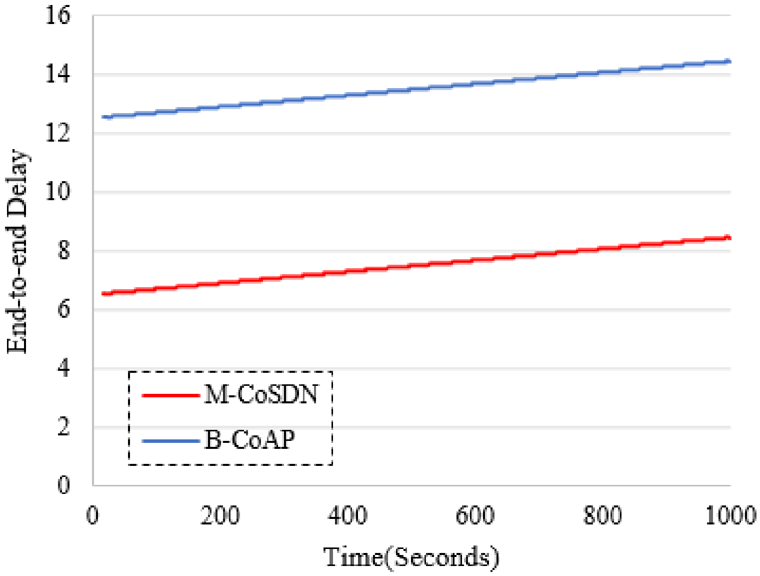


Fig. 9. End-to-End Delay within the Proposed and the basis Algorithm.

Within the basic algorithm, during mobile sensor nodes transmission, the user receives a ‘Destination Inaccessibility Message’ that informs him of the ongoing transmission. Then, the user finds the node’s location through the retransmission of the source discovery message. This process leads to transmission delays. While within the proposed model, the mobile sensor node informs the controller of the domain change using the network. Therefore, the controller can reduce the delays to a bare minimum by updating the current tables and sending them to the network routes. Increasing the simulation time contributes to more delays within both algorithms. The increasing traffic load and transmitted packets within the network cause queuing delays in nodes and other network entities. That is why the End-to-End Delay is bound to increase with time.

Fig. 10 compares network throughput within the two models. In this study, we defined network throughput as the number of successful requests divided by the total number of requests. As observed in Fig. 10, the network throughput in the proposed model is higher than the basic algorithm. The number of signaling messages transmitted between the two entities that might cause delays or collisions within the channel contribute to the higher network throughput in the proposed model. At the beginning of the simulation phase, network throughput was increasing at a high pace. However, with the increasing network traffic loads that cause collisions and errors within the channel, network throughput is decreased at a moderated pace. Therefore, network throughput is dependent on the channel type, errors, and network traffic load.

Fig. 11 demonstrates the network traffic load within the proposed and basic algorithms. As demonstrated in Fig. 11, in the basic algorithm, because of the repeated source discovery within each transmission, the exchanged traffic load increases. As predicted, increasing the simulation time leads to an increased network traffic load in the basic algorithm compared with the proposed algorithm that follows a higher positive slope. Traffic load increase, in turn, leads to increased delays and packet loss within the network. Therefore, network traffic load can impact network throughput and overall productivity.

In this part of the research, we have conducted a study on inter-domain routing. To do so, we have used two different domains controlled by two controllers within the network topology. Furthermore, a new entity called ‘location server’ is added to the network that records the data related to all network sensor nodes. First, the network’s End-to-End Delay is studied (Fig. 12).

It is observed that inter-domain routing imposes more delays than intra-domain routing. However, by comparing Fig. 12 with Fig. 9, it is observed that inter-domain routing within the proposed model imposes much fewer delays than the basic algorithm. Both networks produce the same traffic load (Fig. 13) since both timeouts and delays are the same.

Fig. 14 demonstrates that inter-domain network throughput is slightly less than intra-domain network throughput. Increased packet delay and packet collisions in the network route decrease the number of successful requests, which, in turn, causes a slight decrease in inter-domain network throughput compared with intra-domain network throughput.

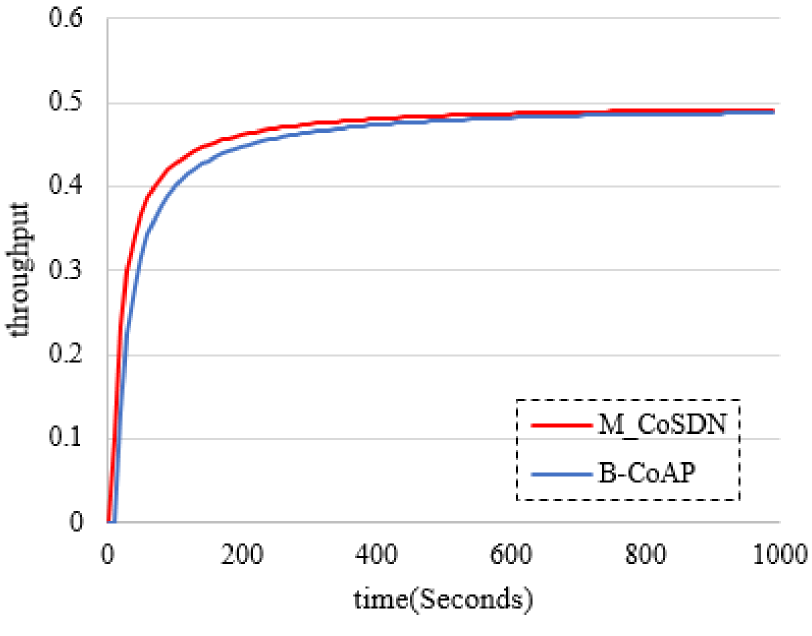


Fig. 10. Network throughput for the Proposed and basis Algorithms.

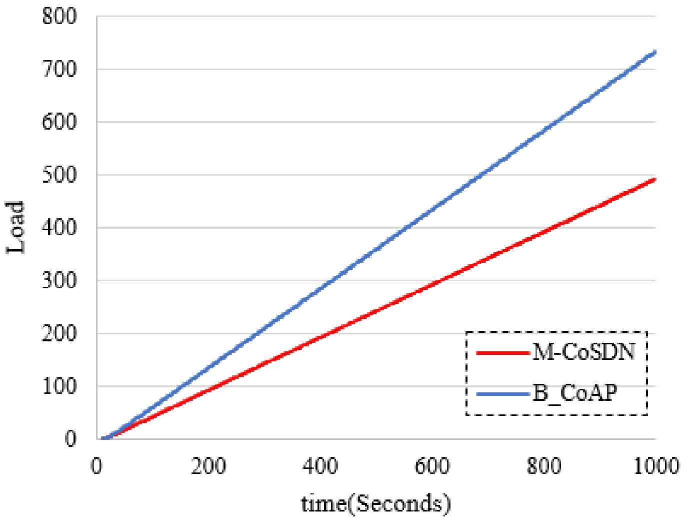


Fig. 11. Network Traffic Load.

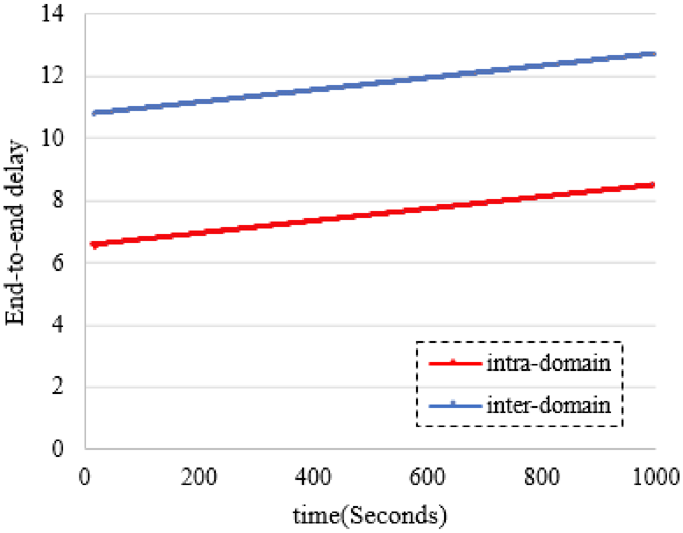


Fig. 12. End-to-End Delay within the Two Inter-Domain and Intra-Domain Scenarios.

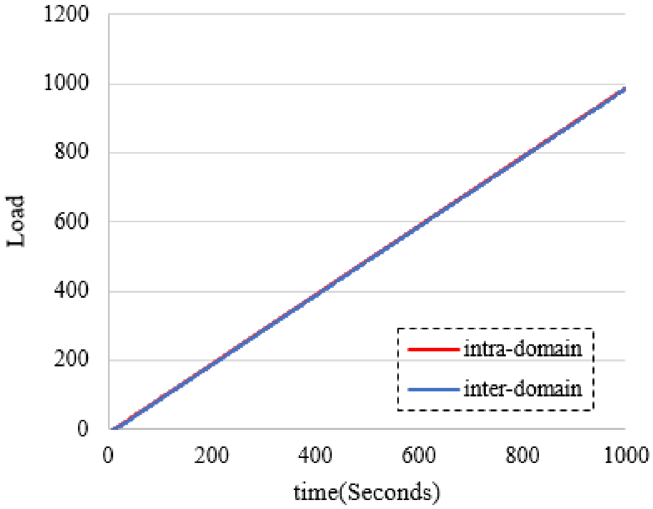


Fig. 13. Network Traffic Load.

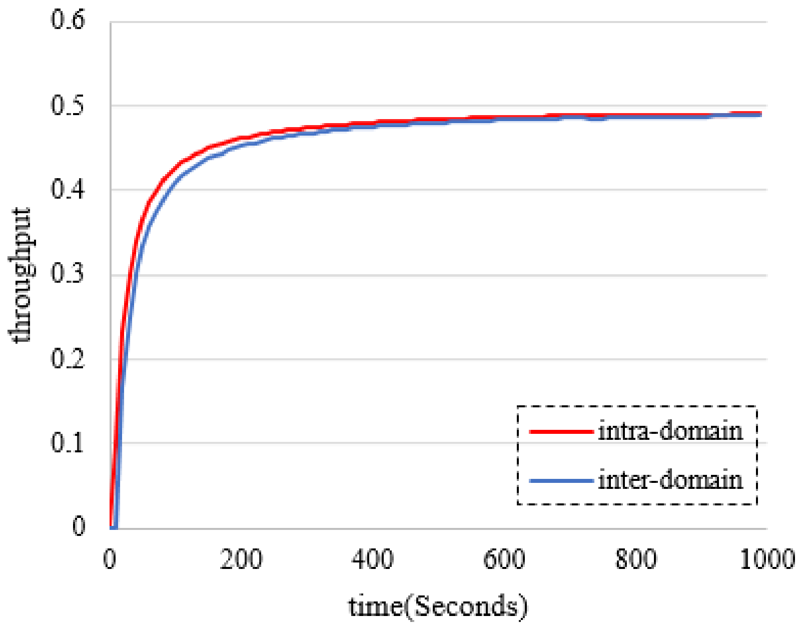


Fig. 14. Two Scenarios for Network throughput.

IV. Conclusion

IoT is a concept that connects multiple devices. The purpose of IoT is to facilitate human life and information exchange. IoT has multiple applications that can impact multiple aspects of human life, including personal, business, and industrial sectors. To increase network flexibility and reduce the costs of sensor nodes' transmission, we need to take a practical approach to the sensor nodes' transmission control. Because of the specific structure, infrastructure, and features of IoT, standard TCPs will not be of use. Therefore, it is essential to introduce a protocol based on the specific features of the IoT.

In this study, a secure M-CoSDN transmission model is introduced that would decrease signaling latency and costs in the IoT ecosystem. The proposed model uses SDN technology to impose centralized control on mobile sensor nodes within the network. CoAP CON messages are used to introduce a secure transmission model. Multicast transmission prevents packet loss and transmission delay for mobile sensors. The efficiency analysis results of the proposed algorithm indicate that it is far more effective than other models.

References

[1] Jeschke, S., Brecher, C., Song, H., & Rawat, D. B. Industrial Internet of Things: Cybermanufacturing Systems. 2017. ISBN-13.

[2] Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., & Zhao, W. (2017). A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. IEEE internet of things journal, 4(5), 1125-1142.

[3] Huang, C., & Huang, Y. (2022). Information Fusion Early Warning of Rail Transit Signal Operation and Maintenance Based on Big Data of Internet of Things. Sustainable Computing: Informatics and Systems, 100763.

[4] Ngu, A. H., Gutierrez, M., Metsis, V., Nepal, S., & Sheng, Q. Z. (2016). IoT middleware: A survey on issues and enabling technologies. IEEE Internet of Things Journal, 4(1), 1-20.

[5] Gazis, V. (2016). A Survey of Standards for Machine-to-Machine and the Internet of Things. IEEE Communications Surveys & Tutorials, 19(1), 482-511.

[6] Zhang, J., Ma, M., Wang, P., & Sun, X. D. (2021). Middleware for the Internet of Things: A survey on requirements, enabling technologies, and solutions. Journal of Systems Architecture, 117, 102098.

[7] Chun, S. M., Kim, H. S., & Park, J. T. (2015). CoAP-based mobility management for the Internet of Things. Sensors, 15(7), 16060-16082.

[8] Braun, W., & Menth, M. (2014). Software-defined networking using OpenFlow: Protocols, applications and architectural design choices. Future Internet, 6(2), 302-336.

[9] Zhou, Q., & Zhang, R. (2013). A survey on All-IP wireless sensor network. In LISS 2012 (pp. 751-756). Springer, Berlin, Heidelberg.

[10] Raza, S. M., Kim, D. S., & Choo, H. (2014, January). Leveraging pmipv6 with sdn. In Proceedings of the 8th International Conference on Ubiquitous Information Management and Communication (pp. 1-8).

[11] Chen, C., Lin, Y. T., Yen, L. H., Chan, M. C., & Tseng, C. C. (2016, April). Mobility management for low-latency handover in SDN-based enterprise networks. In 2016 IEEE wireless communications and networking conference (pp. 1-6). IEEE.

[12] Ghaleb, S. M., Subramaniam, S., Zukarnain, Z. A., & Muhammed, A. (2016). Mobility management for IoT: a survey. EURASIP Journal on Wireless Communications and Networking, 2016(1), 1-25.

[13] Zhang, G., & Navimipour, N. J. (2022). A comprehensive and systematic review of the IoT-based medical management systems: Applications, techniques, trends and open issues. Sustainable Cities and Society, 103914.

[14] Sheng, Z., Yang, S., Yu, Y., Vasilakos, A. V., McCann, J. A., & Leung, K. K. (2013). A survey on the ietf protocol suite for the internet of things: Standards, challenges, and opportunities. IEEE wireless communications, 20(6), 91-98.

[15] Yugha, R., & Chithra, S. (2020). A survey on technologies and security protocols: Reference for future generation IoT. Journal of Network and Computer Applications, 169, 102763.

[16] Makaya, C., & Pierre, S. (2008). An analytical framework for performance evaluation of IPv6-based mobility management protocols. IEEE Transactions on wireless communications, 7(3), 972-983.