01 Jan 2022

An Icn-Based Secure Task Cooperation Scheme in Challenging Wireless Edge Networks

Ningchun Liu

Shuai Gao

Teng Liang

Xindi Hou

et. al. For a complete list of authors, see https://scholarsmine.mst.edu/comsci_facwork/1246

Recommended Citation

N. Liu et al., "An Icn-Based Secure Task Cooperation Scheme in Challenging Wireless Edge Networks," *Proceedings - International Conference on Computer Communications and Networks, ICCCN*, Institute of Electrical and Electronics Engineers, Jan 2022.
The definitive version is available at https://doi.org/10.1109/ICCCN54977.2022.9868864

An ICN-based Secure Task Cooperation Scheme in Challenging Wireless Edge Networks

Ningchun Liu*, Shuai Gao*, Teng Liang†, Xindi Hou*, Sajal K. Das‡

*School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing, China
†Department of New Networks, Peng Cheng Laboratory, Shenzhen, China
‡Department of Computer Science, Missouri University of Science & Technology, Rolla, USA
Email: {nchliu, shgao, freezerburn}@bjtu.edu.cn, liangt@pcl.ac.cn, sdas@mst.edu

2022 International Conference on Computer Communications and Networks (ICCCN) | 978-1-6654-9726-8/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICCCN54977.2022.9868864

***Abstract*—Task cooperation is an effective way to execute a complex task in challenging wireless edge networks. Existing TCP/IP-based solutions encounter the problem of low network resource utilization and the heavy dependency of infrastructure connections. Information-centric networking(ICN) is a promising architecture to address these issues. In existing ICN-based task cooperation schemes, the data reuse feature of ICN improves the utilization of network resources, which also brings potential security threats to the reused data. To guarantee the security of data reuse in task cooperation without affecting the data reuse feature, we propose an ICN-based secure task cooperation scheme. In our scheme, the specific naming convention is designed to support task cooperation and the acquisition of keys. In addition, our scheme implements fine-grained access control for data reuse in task cooperation combined with attribute-based encryption. Experimental results show that our scheme enhances the security of task cooperation with low cost compared with existing schemes.**

***Index Terms*—Task cooperation, attribute-based encryption, ICN, wireless edge networks**

I. Introduction

In recent years, IoT devices have been widely used in various kinds of challenging scenarios, such as military strikes, disaster relief and so on [1]. In the above scenarios, multiple IoT devices with limited resources constituting the wireless edge network need to perform tasks cooperatively, due to the complexity of tasks [2]. However, most wireless edge networks adopt TCP/IP network architecture, which was designed for static hosts and routers connected by wired links. It is difficult to take the advantages of broadcast nature of wireless channels [3]. In addition, the network infrastructure in the challenging scenarios may be partially disabled. In such scenarios there is no guarantee that a fully connected path between source and destination exist at any time, rendering conventional client-server protocols unable to support communication [4].

As a promising network architecture, ICN [5] adopts the content-centric communication model, and supports asynchronous transmission of content between two nodes without maintaining an end-to-end connection, which is considered to be an appropriate network architecture to address above issues in intermittently connected challenging scenarios [6]. In addition, due to the characteristic of in-network caching, ICN can also achieve better efficiency in wireless edge networks by data reuse [7].

To date, some ICN-based schemes [7]–[9] are proposed to improve the resource utilization of wireless edge networks by data reuse. However, these schemes do not take reused data protection into account, which is vulnerable to security threats, such as eavesdropping attacks, unauthorized access control attacks and so on. Other research efforts designed some data protection mechanisms in ICN-based wireless edge networks, which can be classified into authentication-based schemes [10], [11] and encryption-based schemes [12], [13]. Nevertheless, these mechanisms can not take advantage of ICN's data reuse feature and support fine-grained access control for reused data in task cooperation. As a prospective study, Zhang *et al.* [14] firstly introduced attribute-based encryption(ABE) to named data networking(NDN), which is the most promising implementation of ICN [15]. Since then, some studies [16], [17] have been devoted to exploring the integration between NDN and ABE. However, existing ABE-based schemes cannot be directly used for securing reused data of task cooperation in ICN-based wireless edge networks, due to changes in communication service model.

To enhance the security of data reuse in task cooperation without affecting the data reuse feature of ICN, we propose an ICN-based secure task cooperation scheme in challenging wireless edge networks. This paper makes the following contributions:

1) We present an ICN-based secure task cooperation model, which quantifies three types of cost of performing collaborative tasks safely in challenging wireless edge networks, including calculation cost, encryption & decryption cost and communication cost.
2) We extend traditional the naming convention of NDN to support the request of collaborative tasks and the acquisition of keys.
3) We design an attribute-based access control policy according to the time and location information of tasks and the privilege of devices, which ensures fine-grained access control for data reuse in ICN-based task cooperation.
4) We implement and evaluate our scheme on ndnSIM platform. Compared with existing schemes, our scheme enhances the security of task cooperation with low cost.

The remainder of this paper is organized as follows. Section

II reviews the related work. Section III presents the example scenario. In Section IV, we introduce requirements, system model and security assumptions. The scheme design is presented in Section V. Several experiments are done in Section VI to evaluate the performance of our scheme. Security analysis and discussion are introduced in Section VII. Finally, we conclude this paper in Section VIII.

II. Related Work

This section reviews the related work on ICN-based wireless edge networks, which can be classified as improving the efficiency of task execution and enhancing the security of the network.

A. Improving Resource Utilization in ICN-based Wireless Edge Networks

Tan *et al.* [7] proposed an NDN-based distributed collaborative task scheduling scheme in mobile ad hoc networks. To improve the efficiency of performing distributed collaborative tasks, the scheme divides the task into subtasks, which can be reused due to the in-network caching characteristics of NDN. In addition, Lee *et al.* [8] designed a computation reuse architecture for future edge systems. The architecture stores previously executed results and reuses them to satisfy newly arrived similar tasks instead of performing computation from scratch, which has the potential to significantly reduce resource utilization and lessen the time needed for the execution of new tasks. Nevertheless, existing schemes rarely consider how to protect against security threats during task cooperation.

B. Enhancing Security in ICN-based Wireless Edge Networks

Oh *et al.* [10] extended the content-centric networking architecture to adapt to military and emergency communications ad hoc network scenarios with high mobility and high packet loss rate. In the above architecture, to decrypt the received data packet, the consumer needs to obtain the key after being authenticated on the gateway of the autonomous domain. Amadeo *et al.* [11] proposed the protocol named Authenticated Named Data Networking at the Edge(ANDNe), in which the content provider needs to dynamically maintain the public key list of legitimate consumers. In [10] and [11], the network entities responsible for authentication are required to be online, which is not suitable for intermittently connected challenging scenarios.

Misra *et al.* [12] designed a data access control mechanism based on threshold secret sharing. In this mechanism, even if the entity undertaking authentication operation is offline, the content producer can still allow legitimate consumers to decrypt the data. However, to decrypt the content produced by different content providers, the consumer needs to save secret shares from different content providers. The additional overhead is a burden for resource-constrained challenging scenarios. Liu *et al.* [13] designed a data access control mechanism, which introduces the pre-calculated and cached auxiliary key block to reduce the retrieval delay of the auxiliary key block and the decryption cost of consumers. Besides, combining a two-dimensional one-way function, the mechanism ensures the uniqueness of the consumer's secret share. Since the entities responsible for authentication do not need to keep online, the above solutions [12], [13] can be applied in intermittently connected challenging scenarios. However, these solutions cannot support the fine-grained access control requirements of data reuse in task cooperation.

As a prospective study, Zhang *et al.* [14] proposed a name-based access control mechanism in NDN. This mechanism firstly introduces attribute-based encryption and released the NAC-ABE library. Since then, some studies [16], [17] have been devoted to exploring the integration between NDN and ABE. However, these schemes cannot be directly used for securing reused data of task cooperation in ICN-based wireless edge networks, due to changes in communication service model.

III. Example Scenario

We present a challenging disaster relief scenario in Fig. 1, which consists of a task requester, rescue vehicles (RVs), cache-enabled routers, and a trusted control center (TCC).

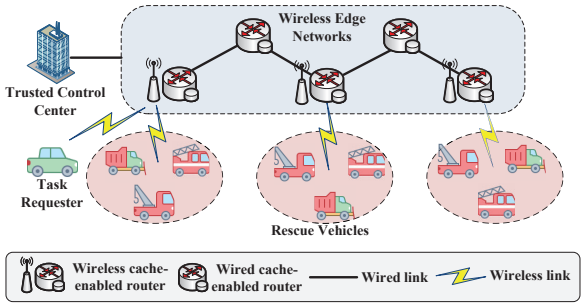


Fig. 1. Disaster relief scenario.

- Task requester reports the emergency event, which contains the emergency event type, location, and time.
- RVs perform rescue tasks cooperatively, including the detection of disaster scenarios and the execution of rescue operations. During task cooperation, RVs may be either content producers or consumers.
- Cache-enabled routers include two types: wired cache-enabled routers and wireless cache-enabled routers. Specifically, wired cache-enabled routers forward the requests and respond to them if the requested contents exist in their cache. In addition to the functions of wired cache-enabled routers, wireless cache-enabled routers can support wireless access.
- TCC can choose a composition of several RVs that perform rescue tasks. In addition, TCC is responsible for the initialization of secure task cooperation and generates the attribute-based access control policy according to the time and location information of tasks and the privilege of RVs.

IV. Requirements, System Model and Security Assumptions

In this section, we firstly analyze the requirements for secure task cooperation in disaster scenarios. Besides, we present the secure task cooperation model to quantify the total cost of performing collaborative tasks safely. In the end, we elaborate the security assumptions in our scheme.

A. Requirements

- **Data confidentiality.** The proposed scheme ensures unauthorized RVs and cache-enabled routers cannot obtain any information from encrypted data in task cooperation.
- **Fine-grained access control.** The scheme guarantees that only RVs that comply with the attribute-based access policy generated by the TCC can access data reused in task cooperation.

B. System Model

We assume that n RVs perform the rescue task cooperatively, and V_i or V_j $(1 \leq i, j \leq n)$ represent one of the RVs. Besides, the rescue task T can be divided into m subtasks, and T_{k-1} and $T_k (1 \leq k-1, k \leq m)$ represent two subtasks executed in sequence. The cost of performing the rescue task T consists of three parts: 1)the calculation cost of the subtask, 2)the encryption and decryption cost of the subtask data, and 3)the communication cost between RVs.

Calculation Cost: The calculation cost of the subtask is determined by the computation capability of the RV performing the subtask and the complexity of the subtask. In addition, if there is a case of data reuse, the calculation cost of the subtask only contains the lookup time of the subtask reuse table. The calculation cost c_k^i is defined as shown in Eq.(1).

$$c_k^i = L_i + (1 - \tau_k^i) \cdot \frac{\Delta_k}{\varphi_i} \tag{1}$$

where c_k^i represents the calculation cost of the V_i performing the subtask T_k, τ_k^i denotes whether the subtask T_k is reused in the V_i ($\tau_k^i = 1$) or not ($\tau_k^i = 0$), L_i refers to the lookup time of the subtask reuse table of V_i, Δ_k represents the complexity of the subtask T_k, and φ_i denotes the computation capability of the V_i.

Encryption & Decryption Cost: Assuming that the length of the content key used for encryption and decryption is 128 bits, the cost of encryption and decryption of subtask data is determined by the encryption and decryption capability of RVs and the size of the input & output data of the subtask. In addition, if there is a case of data reuse, the encryption cost of the subtask output data is zero. The encryption and decryption cost s_k^i is defined as shown in Eq.(2).

$$s_k^i = \frac{I_k}{\beta_i \cdot \varphi_i} + (1 - \tau_k^i) \cdot \frac{O_k}{\alpha_i \cdot \varphi_i} \tag{2}$$

where s_k^i represents the encryption and decryption cost of the V_i performing the subtask T_k, I_k refers to the input data size of subtask T_k, O_k denotes the output data size of subtask T_k, α_i represents the encryption ability coefficient of V_i, and β_i refers to the decryption ability coefficient of V_i.

Communication Cost: The communication cost between RVs is determined by the size of the input & output data of the subtask and the bandwidth between RVs. Since NDN adopts a "pull"-based communication paradigm, the communication cost consists of the transmission delay of the Interest packet and the Data packet. The communication cost $d_{k,k+1}^{i,j}$ is defined as shown in Eq.(3).

$$d_{k-1,k}^{j,i} = \frac{I_k + O_k}{b_{j,i}} \tag{3}$$

where $d_{k-1,k}^{j,i}$ denotes the communication cost between V_j executing subtask T_{k-1} and V_i executing subtask T_k, and $b_{j,i}$ refers to the bandwidth between V_j and V_i.

The objective function is shown in Eq.(4), which tends to minimize the overall task's execution cost.

$$\min_{T_k \in T} \sum_{k=1}^{m} (d_{k-1,k}^{j,i} + s_k^i + c_k^i) \tag{4}$$

C. Security Assumptions

1) Rescue Task: Considering that the rescue task in disaster scenarios are usually more complicated. It is difficult for a single rescue vehicle to complete a complex rescue task alone due to its limited resources. We assume that the rescue task is splittable. Specifically, subtasks divided by the rescue task can be executed cooperatively at different rescue vehicles, and there is a sequential relationship between subtasks(Specifically, the output of the previous subtask will be the input of the next subtask).

2) RVs: In our scheme, RVs are assumed to be malicious. On the one hand, they try to destroy unauthorized data through eavesdropping or tampering. On the other hand, they may collide with each other, or even collude with cache-enabled routers to launch the above attacks.

3) Cache-enabled routers: Cache-enabled routers located in disaster scenarios can provide cached data of rescue tasks for RVs. We assume that cache-enabled routers are rational and curious. By rational, we mean that, cache-enabled routers will comply with designated protocols that provide services for RVs. By curious, we mean that cache-enabled routers may be curious about the rich information in cached data. For example, they may be interested in when and where the disaster event occurred, which will pose a potential threat to disaster relief.

4) TCC: As a management and control agency for disaster relief, the TCC is trusted in our scheme.

V. Scheme Design

In this section, we describe the naming convention of our scheme in Section V-A. In addition, the workflow of our scheme is shown in Section V-B.

A. Naming Convention

In this section, we design the specific naming convention for secure task cooperation. All the task request packets and key-related packets in our scheme follow the convention.

1) Task Request: In task cooperation, RVs execute subtasks in sequence according to the execution order set by the TCC. In the process of performing tasks, an RV needs to send a task request packet. The name convention of the task request packet is defined as follows.

$$\begin{aligned}\text{Task Request Name} = \text{“/}&\langle\text{TCC prefix}\rangle\text{/STC/}\langle\text{subtask prefix}\rangle\\ &\text{/PARAM/}\langle\text{parameter}\rangle\\ &\text{/SUBTASK/}\langle\text{subtask prefix i}\rangle\text{”}\end{aligned}$$

where the TCC prefix refers to the entity that orchestrates the rescue task, the subtask prefix is the name prefix of the subtask split by rescue task, the parameter is the input parameter of the subtask, and the subtask prefix i is the name prefix of the additional subtasks in rescue task.

2) Encryption Key (EK): In secure task cooperation, an RV needs to fetch the EK packet and decrypt it to get the CK packet. The naming convention of the EK packet is defined as follows.

$$\begin{aligned}\text{EK Interest Name} = \text{“/}&\langle\text{TCC prefix}\rangle\text{/STC/}\langle\text{subtask prefix}\rangle\text{”}\\ \text{EK Data Name} = \text{“/}&\langle\text{TCC prefix}\rangle\text{/STC/}\langle\text{subtask prefix}\rangle\\ &\text{/ENCRYPTED-BY/}\langle\text{attribute policy}\rangle\text{”}\end{aligned}$$

where the TCC prefix indicates the name prefix of the TCC which generates the EK, the subtask prefix is the name prefix of the subtask executed by the RV, the attribute policy indicates the granularity of the data.

3) Attribute Key (AK): To decrypt the EK packet, an RV needs to fetch the AK packet from the TCC. The naming convention of the AK packet is defined as follows.

$$\begin{aligned}\text{AK Interest name} = \text{“/}&\langle\text{TCC prefix}\rangle\text{/ATTRIBUTE/}\langle\text{attribute name}\rangle\text{”}\\ \text{AK Data name} = \text{“/}&\langle\text{TCC prefix}\rangle\text{/ATTRIBUTE/}\langle\text{attribute name}\rangle\\ &\text{/ENCRYPTED-BY/}\langle\text{RV prefix}\rangle\text{”}\end{aligned}$$

4) Content Key (CK): To encrypt(or decrypt) the data of subtasks, an RV needs to fetch the CK packet, which is encrypted by the EK. The naming convention for the CK packet is defined as follows.

$$\begin{aligned}\text{CK Interest Name} = \text{“/}&\langle\text{TCC prefix}\rangle\text{/STC/}\langle\text{subtask prefix}\rangle\\ &\text{/CK/}\langle\text{CK-id}\rangle\text{”}\\ \text{CK Data Name} = \text{“/}&\langle\text{TCC prefix}\rangle\text{/STC/}\langle\text{subtask prefix}\rangle\\ &\text{/CK/}\langle\text{CK-id}\rangle\text{/ENCRYPTED-BY/}\langle\text{EK name}\rangle\text{”}\end{aligned}$$

B. Workflow

The workflow of our scheme consists of four steps, as shown in Fig. 2. The first three steps are performed at the TCC. The fourth step occurs in RVs, which requires task cooperation between RVs.

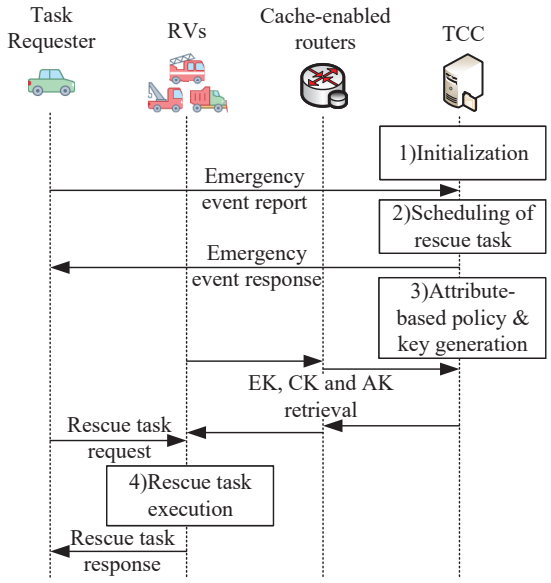


Fig. 2. Workflow of secure task cooperation.

1) Initialization: In this step, the TCC firstly generates the public parameter PK and the master secret key MSK. Then, the MSK needs to be distributed to legitimate RVs.

2) Scheduling of Rescue Task: When a disaster occurs, the task requester will send the emergency event report to the TCC. After receiving this report, the TCC selects the optimal set of RVs to perform the rescue task according to the location of the disaster event and the computation capability of RVs.

3) Attribute-based Policy & Key Generation: After choosing the appropriate set of RVs, the TCC needs to generate an attribute-based access control policy Γ, which contains the time and location information of tasks and the privilege of RVs, as shown in Fig. 3.

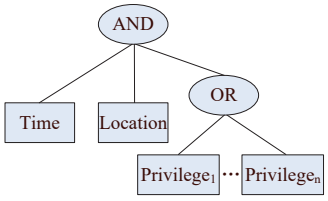


Fig. 3. Attribute-based access control policy.

Then, the TCC generates the EK by using the CP-ABE algorithm, which takes the public parameter PK and the attribute-based access control policy Γ as input parameter.

Finally, the TCC needs to generate attribute keys for each V_i by using the key generation algorithm, which takes the public parameter PK, the master secret key MSK, and the attribute set of RVs as input parameter.

In our scheme, RVs need to send Interest packet that follows specific naming conventions to obtain keys periodically.

4) Rescue Task Execution: In this step, RVs which comply with attribute policy Γ will execute subtasks in sequence scheduled by the TCC. In addition, we present the processing flow of subtask executing in a single RV, and show how to ensure the confidentiality of data between RVs in task cooperation.

Algorithm 1: The processing flow of subtask in V_i

Input: I_k: Input data of T_k.
Output: O_k: Output data of T_k.

```
if T_k ∈ T then
    Input=I_k.Decrypt();
    Flag=SubtaskReuseTable.query(Prefix,Input);
    if Flag≠ ∅ then
        O_k=SubtaskReuseTable.output();
    else
        Output=T_k.compute(Input);
        O_k=Output.Encrypt();
        SubtaskReuseTable.add(Prefix,Input, O_k);
    end
    return O_k;
end
Forward T_k to other RVs;
```

The processing flow of subtasks in RVs is shown in Algorithm 1. When the rescue vehicle V_i that conforms to the attribute policy Γ receives the task request of the subtask T_k, the V_i decrypts the input data in the task request. Then, the V_i needs to query the local subtask table according to the subtask prefix and input data. If there is a hit in the local subtask reuse table, the output result will be encrypted and returned. Otherwise, the V_i determines whether the local computation capability meets the complexity requirements of the subtask. If it is satisfied, the V_i executes the subtask T_k. Then, the output result will be encrypted and returned. Otherwise, the subtask request is forwarded to other RVs.

We present secure data reuse in RVs in Fig. 4. In our scheme, V_i needs to use its attribute key AK_i to decrypt and obtain the content key CK by using decryption algorithm, which takes the public parameter PK, the encryption key EK, and the attribute key AK_i as input parameter.

Finally, V_i will encrypt the output data and send the subtask request to V_{i+1} which executes the next subtask. After receiving the subtask request, V_{i+1} will process the subtask request (in Algorithm 1) to execute the next subtask in sequence.

VI. Performance Evaluation

In this section, we firstly implement the proposed scheme. Then, we evaluate the performance of the scheme proposed in this paper.

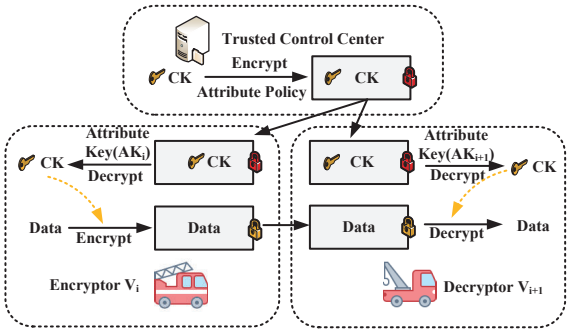


Fig. 4. Secure data reuse in RVs.

A. Experimental Environment

First, using the NAC-ABE library[1], we implement the described attribute-based secure task cooperation scheme. Then, we use ndnSIM [18] to simulate our scheme integrated with standard NDN. We implemented a proof of concept of our scheme with four entities containing TCC, task requester, cache-enabled routers, and RVs. The task requester sends the emergency event report to the TCC. After receiving the message, the TCC selects the optimal set of RVs based on the available resources in RVs. Then, RVs perform tasks cooperatively under the dispatch of the TCC.

Considering that the TCC is usually located at the rear, we set the transmission delay and link bandwidth of the link between TCC and the wireless edge network to 100ms and 10Mbps respectively. In addition, the transmission delay and link bandwidth of the link between any cache-enabled routers are set to 10ms and 100Mbps respectively. In the simulation, task requesters issue 100 tasks, and each task consists of any three subtasks. Table. I provides a summary of the used parameters. All the experiments are conducted on a Linux system(Ubuntu 16.04) with a 3.40GHz Intel) Core i7-3770 processor and 16G RAM.

TABLE I
Experimental Parameter.

Parameter	Value
Number of RVs	[5-50]
Number of tasks	100
Number of subtasks	300
Tasks arrival rate	5 tasks per second
Replacement policy	LRU

B. Experimental Results and Analysis

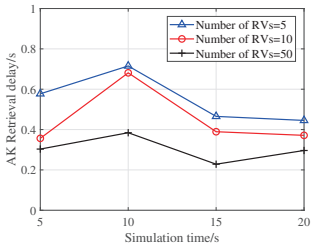
We evaluate the performance of the proposed scheme from the following metrics:(1) average key retrieval delay, (2) subtask reuse rate, and (3) total execution time of rescue task.

[1]https://github.com/UCLA-IRL/NAC-ABE/

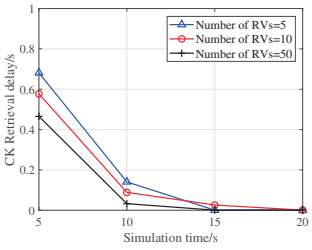
1) Average Key retrieval delay: To guarantee the security of data reuse in task cooperation, we additionally introduced three types of keys containing Attribute Key(AK), Content Key(CK), and Encryption Key(EK). Fig. 5 displays the key retrieval delay of RVs for obtaining three types of keys separately in different numbers of RVs.

Fig. 5(a) shows that the average retrieval delay of AK has little change with the increase of simulation time. Because each RV has a specific AK, the in-network caching almost does not affect the retrieval delay of AK. In addition, the retrieval delay of AK decreases with the increase in the number of RVs. Due to the increase in vehicle density, the connection opportunities between RVs increase, and the number of data packet retransmissions decreases. Since AK is usually obtained at the beginning of task cooperation, which has a slight impact on our scheme.

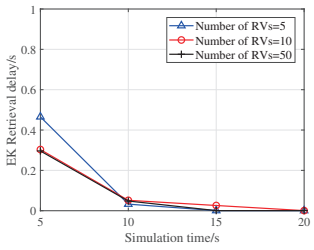
Fig. 5(b) and Fig. 5(c) show that the average retrieval delay of EK and CK. Due to the effect of the in-network caching, the retrieval delay of EK and CK reduce rapidly with the increase of simulation time respectively in different numbers of RVs, which means that the cost of RVs for obtaining three types of keys introduced by our scheme is low.



(a) Attribute Key.



(b) Content Key.



(c) Encryption Key.

Fig. 5. Key retrieval delay.

2) Subtask reuse rate: Fig. 6 shows the subtask reuse rate in different numbers of RVs, and the subtask reuse rate refers to the ratio between the number of subtasks that results are reused and the total number of subtasks. The subtask reuse rate is positively correlated with the simulation time. In the case of the same time, the more vehicles there is the higher the subtask reuse rate. That is to say, the increase in the number of RVs helps improve the efficiency of task execution.

3) Total task execution time: Fig. 7 displays a comparison among the traditional scheme, the scheme proposed by Tan *et al.* [7], the dummy scheme, and the proposed scheme in total execution time of task cooperation.

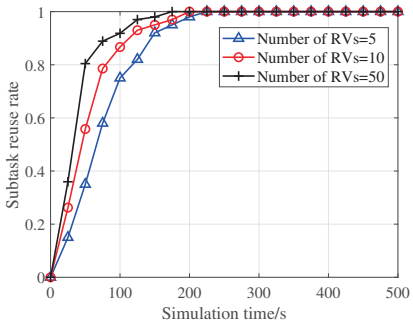


Fig. 6. Subtask reuse rate.

- **Traditional Scheme.** Neither considering the reuse of subtasks, nor protecting task data.
- **Tan *et al.* Scheme.** Only considering the reuse of subtasks.
- **Dummy Scheme.** Considering the reuse of subtasks and protecting task data with RSA and AES encryption algorithm.
- **Proposed scheme.** Considering the reuse of subtasks and protecting task data with CP-ABE and AES encryption algorithm.

The result shows that the proposed scheme can reduce the total execution time compared with the traditional scheme, and the total execution time is saved by 54.44% owing to the reuse of subtasks. Compared with the dummy scheme, the proposed scheme also reduces the total execution time due to the reduction of cryptographic operations. The total execution time is saved by 44.67% than the dummy scheme. In addition, compared with the Tan *et al.* scheme, the proposed scheme introduces a slight time overhead due to security cost, the total execution time is increased by 6.81%.

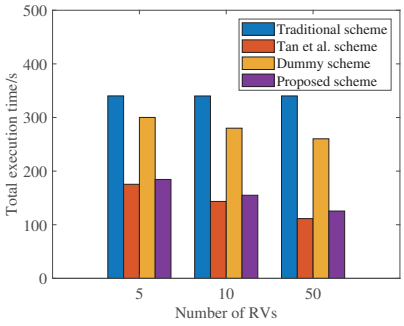


Fig. 7. Total execution time.

VII. Security Analysis and Discussion

In this section, we explain how our scheme mitigates potential threats containing eavesdropping attacks and unauthorized access control attacks. In addition, we evaluate the security cost of our scheme.

A. Data Confidentiality

In eavesdropping attacks, attackers may sniff on the broadcast channel or obtain Data packets of rescue tasks from in-network caching. Nevertheless, attackers cannot understand what ciphertext represents because all the sensitive content(e.g., input data of subtasks, output data of subtasks, and CK) are encrypted.

B. Fine-grained Access Control

In unauthorized access control attacks, legitimate RVs may retrieve data beyond the limits of their access privileges. However, the TCC can ensure fine-grained access control by restricting the granularity of authorized RVs in our scheme. For example, EK *"/urban/control/STC/rescue task/ENCRYPTED-BY/*$Time_1$ *AND* $Location_1$ *AND (*$Privilege_1$ *OR* $Privilege_2$*)"* is used to encrypt CK. By using specific attribute policy, Data packet produced under the EK cannot be decrypted by RVs which are located in $Location_2$ or with another privilege $Privilege_3$.

C. Security Cost Evaluation

We evaluate the cryptographic operations in our scheme. Assuming we have L RVs and M tasks with different granularities which consist of N subtasks in task cooperation, there are $M \times N$ content Data packets. In a traditional solution based on the RSA algorithm, we let each RV has access right to all $M \times N$ content Data packets of subtasks. In our scheme, we assume that each RV has all a attributes. The cryptographic operations are listed as Table II. Compared with traditional solutions based on RSA, the proposed scheme has a smaller number of cryptographic operations, due to the data reuse of subtasks.

TABLE II
THE COMPARISON OF CRYPTOGRAPHIC OPERATIONS BETWEEN DUMMY SCHEME AND PROPOSED SCHEME.

Functional Entity	Dummy Scheme (with RSA)	Proposed scheme (with CP-ABE)
Trusted Control Center	RSA Key Gen: M RSA Enc: L×M AES Enc: L×M	CP-ABE Key Gen: a CP-ABE Enc: a×L[1] AES Enc: M
Rescue Vehicles	RSA Dec: L×M AES Enc: M×N AES Dec: M×N	CP-ABE Dec: L×M AES Enc: M×N^2 AES Dec: M×N^2

[1] M×N can be reduced significantly because of the reuse of subtasks.

VIII. Conclusion

In this paper, we propose an ICN-based secure task cooperation scheme in challenging wireless edge networks. Combined with attribute-based encryption, our scheme can achieve fine-grained access control for data reuse in task cooperation. Experimental results show that our scheme enhances the security of task cooperation with low cost compared with existing schemes.

Acknowledgment

This work was supported by the National Key Research and Development Program of China (No. 2019YFB1802503), the National Nature Science Foundation of China (No. 61972026).

References

[1] M. Mozaffari, W. Saad, M. Bennis, and M. Debbah, "Mobile unmanned aerial vehicles (uavs) for energy-efficient internet of things communications," *IEEE Transactions on Wireless Communications*, vol. 16, no. 11, pp. 7574–7589, 2017.

[2] Z. Zheng, A. K. Sangaiah, and T. Wang, "Adaptive communication protocols in flying ad hoc network," *IEEE Communications Magazine*, vol. 56, no. 1, pp. 136–142, 2018.

[3] M. Meisel, V. Pappas, and L. Zhang, "Ad hoc networking via named data," in *Proceedings of the fifth ACM international workshop on Mobility in the evolving internet architecture*, pp. 3–8, 2010.

[4] T. Liang, J. Pan, and B. Zhang, "Ndnizing existing applications: Research issues and experiences," in *Proceedings of the 5th ACM Conference on Information-Centric Networking*, pp. 172–183, 2018.

[5] B. Ahlgren, C. Dannewitz, C. Imbrenda, D. Kutscher, and B. Ohlman, "A survey of information-centric networking," *IEEE Communications Magazine*, vol. 50, no. 7, pp. 26–36, 2012.

[6] S. Arshad, M. A. Azam, M. H. Rehmani, and J. Loo, "Recent Advances in Information-Centric Networking-Based Internet of Things (ICN-IoT)," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2128–2158, 2019.

[7] X. Tan, Y. Jin, W. Feng, S. Wang, and Y. Yang, "Scheduling of distributed collaborative tasks on ndn based manet," in *Proceedings of the ACM SIGCOMM 2019 Workshop on Mobile AirGround Edge Computing, Systems, Networks, and Applications*, MAGESys'19, (New York, NY, USA), p. 36–42, Association for Computing Machinery, 2019.

[8] J. Lee, A. Mtibaa, and S. Mastorakis, "A case for compute reuse in future edge systems: An empirical study," in *2019 IEEE Globecom Workshops (GC Wkshps)*, pp. 1–6, IEEE, 2019.

[9] B. Nour and S. Cherkaoui, "A network-based compute reuse architecture for iot applications," *arXiv preprint arXiv:2104.03818*, 2021.

[10] S. Y. Oh, D. Lau, and M. Gerla, "Content centric networking in tactical and emergency manets," in *2010 IFIP Wireless Days*, pp. 1–5, 2010.

[11] M. Amadeo, C. Campolo, A. Molinaro, C. Rottondi, and G. Verticale, "Securing the mobile edge through named data networking," in *2018 IEEE 4th World Forum on Internet of Things (WF-IoT)*, pp. 80–85, 2018.

[12] S. Misra, R. Tourani, F. Natividad, T. Mick, N. E. Majd, and H. Huang, "Accconf: An access control framework for leveraging in-network cached data in the icn-enabled wireless edge," *IEEE Transactions on Dependable and Secure Computing*, vol. 16, no. 1, pp. 5–17, 2019.

[13] L. Ning-Chun, G. Shuai, H. Xin-Di, and G. Xin-Chang, "A data access control scheme in information-centric mobile ad hoc networks," *Journal of Beijing University of Posts and Telecommunications*, vol. 44, no. 02, pp. 54–60, 2021.

[14] Z. Zhang, Y. Yu, S. K. Ramani, A. Afanasyev, and L. Zhang, "Nac: Automating access control via named data," in *MILCOM 2018 - 2018 IEEE Military Communications Conference (MILCOM)*, pp. 626–633, 2018.

[15] L. Zhang, A. Afanasyev, J. Burke, V. Jacobson, K. Claffy, P. Crowley, C. Papadopoulos, L. Wang, and B. Zhang, "Named data networking," *ACM SIGCOMM Computer Communication Review*, vol. 44, no. 3, pp. 66–73, 2014.

[16] L. Wang, Z. Zhang, M. Dong, L. Wang, Z. Cao, and Y. Yang, "Securing named data networking: Attribute-based encryption and beyond," *IEEE Communications Magazine*, vol. 56, no. 11, pp. 76–81, 2018.

[17] S. K. Ramani, R. Tourani, G. Torres, S. Misra, and A. Afanasyev, "Ndn-abs: Attribute-based signature scheme for named data networking," in *Proceedings of the 6th ACM Conference on Information-Centric Networking*, pp. 123–133, 2019.

[18] S. Mastorakis, A. Afanasyev, and L. Zhang, "On the evolution of ndnsim: An open-source simulator for ndn experimentation," *ACM SIGCOMM Computer Communication Review*, vol. 47, no. 3, pp. 19–33, 2017.