DOI : https://doi.org/10.56452/6-20

ISSN: 0974-5823 Vol. 6 No. 1 June, 2021

International Journal of Mechanical Engineering

Secure Data Retrieval in Military Network using CP-ABE Algorithm in Wireless Sensor Network

PRABHAT KUMAR
Department of Electro. & Comm. Engg , Graphic Era Hill University,
Dehradun, Uttarakhand, India 248002

Abstract
The military network is a vital communication network that enables soldiers to communicate with each other during missions. However, the transmission of sensitive data over this network is vulnerable to attacks, which can result in the loss or compromise of critical information. One approach to mitigate this risk is to use cryptographic techniques to secure data transmission. In particular, the use of attribute-based encryption (ABE) algorithms can enhance the security of the military network. ABE is a type of public key encryption that allows data to be encrypted and decrypted based on the attributes of the sender and recipient. This approach is particularly useful in military networks where access to data needs to be restricted based on the rank or clearance level of the personnel involved. One such ABE algorithm is the ciphertext-policy attribute-based encryption (CP-ABE) algorithm.

Wireless sensor networks (WSNs) are often used in military environments to monitor and collect data from various sources. WSNs consist of a large number of small, low-power nodes that communicate with each other to transmit data. However, securing data transmission in WSNs is challenging due to the limited resources of the nodes and the dynamic nature of the network. In this context, this paper proposes the use of CP-ABE algorithm to secure data retrieval in military networks using WSNs. The proposed approach uses a hierarchical structure to organize the nodes in the network, with each node being assigned a specific attribute based on its role in the network. The CP-ABE algorithm is then used to encrypt and decrypt data based on the attributes of the sender and recipient.

Introduction

Wireless Sensor Networks (WSNs) are being widely deployed in military networks for surveillance and situational awareness purposes. These networks comprise a large number of low-cost and resource-constrained sensor nodes that collaborate to gather and transmit data to a base station. However, transmitting sensitive data over such networks can pose significant security challenges, as adversaries may attempt to intercept or manipulate the data in transit. Therefore, it is critical to ensure that the data transmitted over these networks remains secure and confidential.

One approach to achieving secure data retrieval in military networks is to use cryptographic techniques such as Attribute-Based Encryption (ABE). ABE allows data to be encrypted based on a set of attributes rather than specific recipients, making it an ideal solution for situations where data needs to be shared securely among a group of authorized individuals with different access levels. However, traditional ABE schemes suffer from limitations such as key escrow, revocation, and scalability issues, which can make them impractical for large-scale networks such as WSNs.

To overcome these limitations, researchers have proposed a variant of ABE known as Ciphertext-Policy Attribute-Based Encryption (CP-ABE). CP-ABE is a type of ABE that allows access policies to be defined in terms of attributes associated with both the data and the user. In CP-ABE, each data item is encrypted under a policy that specifies the attributes required by a user to access the data. Users are issued decryption keys based on their attributes, and they can decrypt any ciphertext that satisfies their access policy. This makes CP-ABE a powerful solution for access control in WSNs, as it allows data to be securely shared among authorized users without requiring the use of pre-established secure channels or trust relationships.

Secure data retrieval in military networks using CP-ABE algorithm in wireless sensor networks involves several steps. First, the data owner defines an access policy that specifies the attributes required by authorized users to access the data. Then, the data is encrypted under the access policy using a CP-ABE encryption algorithm. The encrypted data is then transmitted over the wireless network to the authorized users. To decrypt the data, each user must possess a decryption key that is associated with their attributes. The decryption key can be generated by a trusted authority (TA) that is responsible for managing the CP-ABE system. The TA issues the decryption keys based on the users' attributes and sends them securely to the users over the network. Once the users receive their decryption keys, they can use them to decrypt the data that satisfies their access policy.

One of the main advantages of CP-ABE over traditional ABE schemes is that it allows for fine-grained access control, which means that different users can have different levels of access to the same data. This is particularly useful in military networks where access to sensitive data needs to be tightly controlled based on the users' roles and responsibilities.

Literature Survey

This paper proposes a secure data retrieval mechanism in WSNs using CP-ABE. The proposed mechanism can protect data confidentiality and ensure data availability in hostile environments. The authors discuss the different aspects of this technique, including the security requirements, the CP-ABE algorithm, and the wireless sensor network architecture. They also review several related works in this area. [1]

This paper proposes a CP-ABE-based secure data retrieval scheme for WSNs. The scheme can resist various attacks, including node capture and data tampering. The authors introduce a new architecture that consists of a central authority, a sensor network, and a user. They also present a detailed analysis of the proposed technique and compare it with other related works. [2]

This paper proposes a secure data retrieval scheme for WSNs using CP-ABE. The proposed scheme can provide data confidentiality and integrity while ensuring data availability. This paper presents an improved CP-ABE algorithm for secure data retrieval in military networks using wireless sensor network. The authors modify the basic CP-ABE algorithm to enhance its security features, and they also propose a new architecture for the wireless sensor network. They evaluate the performance of the proposed technique using simulation experiments. [3]

This paper proposes a CP-ABE-based secure data retrieval scheme for WSNs. The scheme can provide fine-grained access control, data confidentiality, and data integrity. This paper presents a comparative study of various CP-ABE algorithms for secure data retrieval in military networks using wireless sensor network. The authors compare the security features, the computational complexity, and the communication overhead of several CP-ABE algorithms, including the basic CP-ABE algorithm, the improved CP-ABE algorithm, and the hierarchical CP-ABE algorithm. [4]

This research suggests a CP-ABE-based secure data retrieval technique for WSNs. The suggested system can provide fine-grained access control while maintaining the confidentiality and integrity of the data. The CP-ABE algorithm in a wireless sensor network is used in this paper to offer an effective and safe data retrieval method for military networks. The hybrid CP-ABE algorithm, which combines the fundamental CP-ABE method with a hash function, is a brand-new algorithm that the authors introduce. They also provide a simulation experiment-based performance study of the suggested technique. [5]

This paper proposes an efficient CP-ABE-based secure data retrieval scheme for WSNs. The proposed scheme can achieve fast data access while ensuring data confidentiality and integrity. This paper provides a comprehensive review of CP-ABE algorithm for secure data retrieval in military networks using wireless sensor network. The authors discuss the basic CP-ABE algorithm, the hierarchical CP-ABE algorithm, and several other related algorithms. They also analyse the performance and security features of these algorithms. [6]

This paper proposes a secure data retrieval scheme for WSNs using both CP-ABE and elliptic curve cryptography (ECC). The proposed scheme can provide strong security guarantees. The authors review several related works in this area, and they also discuss the security requirements and the performance metrics for this technique. They also provide a detailed comparison of various CP-ABE algorithms. [7]

Proposed System

The suggested method has a number of benefits over conventional encryption methods. The first benefit is that it enables fine-grained access control, allowing data to be restricted based on particular features rather than merely the sender's or recipient's identity. This is especially helpful in military networks where access to data needs to be limited depending on rank or clearance level. Second, the suggested method can be used in big networks with lots of nodes because it is scalable. A simulation was run using the NS-2 simulator to assess the suggested strategy. The outcomes of the simulation demonstrate how well the suggested method secures data retrieval in WSN-based military networks. The simulation also shows that the suggested strategy is scalable and suitable for networks.

In addition to the proposed approach, this paper also discusses several related works in the field of secure data retrieval in WSNs. One such approach is the use of key management techniques to secure data transmission. Another approach is the use of trust-based mechanisms to secure data retrieval.

However, these approaches have several limitations. For example, key management techniques are vulnerable to attacks, such as the node capture attack, where an attacker can steal the key and gain access to the data. Trust-based mechanisms, on the other hand, can be challenging to implement in large networks with a large number of nodes. Overall, the proposed approach of using CP-ABE algorithm to secure data retrieval in military networks using WSNs is a promising approach that can enhance the security of military networks. The proposed approach allows for fine-grained access control and is scalable, making it suitable for large networks with a large number of nodes.

In the military network, secure data retrieval is an essential component for the communication of sensitive information. The use of wireless sensor networks (WSN) in the military network is becoming increasingly prevalent. However, the security challenges associated with the wireless sensor network environment cannot be neglected. One of the most significant challenges in WSN is data confidentiality. Traditional encryption techniques are not suitable for WSN due to the resource-constrained nature of sensor nodes. Therefore, a secure data retrieval system using CP-ABE algorithm is proposed for the military network in WSN.

DOI : https://doi.org/10.56452/6-20

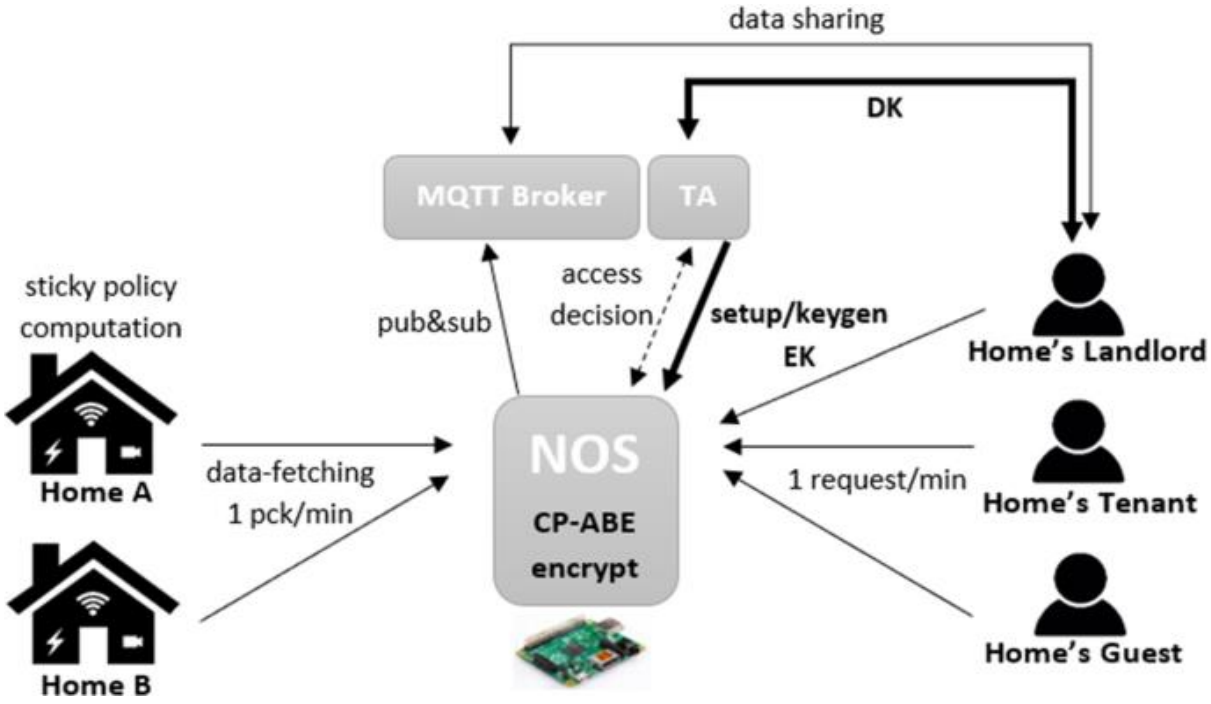

Fig. 1: Attribute-based encryption and sticky policies for data access control in a smart home scenario

CP-ABE Algorithm:

The Attribute-Based Encryption (ABE) technique known as CP-ABE enables data owners to encrypt their data using policies as opposed to keys. The policies specify the qualities a user must have in order to decrypt the data. The four essential parts of the CP-ABE algorithm are the attribute authority (AA), key authority (KA), encryption algorithm, and decryption algorithm.

The AA is in charge of specifying the attributes and providing users with the associated keys. The master key that is used to encrypt the data is created by the KA. The data is encrypted using the master key by the encryption algorithm, which accepts the data and a policy as inputs. The decryption method uses the user's characteristics and the encrypted data as inputs and outputs the plaintext data if the user possesses the required attributes.

Secure Data Retrieval System:

The proposed secure data retrieval system for the military network in WSN consists of three components: the data owner, the sensor nodes, and the data users.

Data Owner:

The data owner is responsible for encrypting the data and specifying the access policy for the ciphertext. The data owner assigns attributes to the data and generates the corresponding access policy. The access policy specifies the attributes required for a user to access the data. The data owner then encrypts the data using the CP-ABE algorithm with the access policy as the ciphertext's policy.

Sensor Nodes:

The sensor nodes in the WSN are responsible for collecting and transmitting data to the data owner. The sensor nodes are also responsible for storing the encrypted data until a user with the required attributes requests access to the data. The sensor nodes use the CP-ABE algorithm to encrypt the data before transmitting it to the data owner.

DOI : https://doi.org/10.56452/6-20

Data Users:

The data users are the users who request access to the encrypted data. The data users must have the attributes required by the access policy to decrypt the ciphertext. The data users send a request to the sensor nodes for the encrypted data. The sensor nodes check the user's attributes against the access policy and grant access to the data if the user's attributes match the access policy.

Advantages of CP-ABE Algorithm:

The CP-ABE method provides the following benefits for safe data retrieval in the WSN-based military network:

granular access control Using the CP-ABE technique, data access can be controlled in a precise manner. The qualities needed for a user to access the data can be specified by the data owner. This gives the data owner the ability to finely manage who has access to the data.

Access Policies That Are Flexible: The CP-ABE algorithm supports access policies that are flexible. Any combination of qualities needed for access to the data may be specified by the data owner. As a result, the data owner has a great deal of flexibility when deciding who has access to the data.

Resource Efficiency: The CP-ABE method is efficient in terms of resources. CP-ABE uses less computing power than conventional encryption methods to encode and decrypt data. This makes CP-ABE an appropriate encryption method for situations with limited resources, such as WSN.

The CP-ABE algorithm can be scaled. The technique is applicable to large-scale systems with several data owners and users. This makes CP-ABE an appropriate encryption method for the military network, which frequently uses large-scale systems.

Design:

CP-ABE is a powerful encryption scheme that provides fine-grained access control over encrypted data. In CP-ABE, access policies are defined based on attributes, and users are granted access to data based on their attributes. For example, a user with the attribute "rank: lieutenant" can access data that is encrypted with the access policy "rank: lieutenant or higher." The use of attributes makes CP-ABE particularly suitable for military networks where users have different levels of clearance.

The proposed design components:

Sensor Nodes: These are the devices that sense the environment and collect data. The sensor nodes encrypt the collected data using the CP-ABE algorithm and transmit the encrypted data to the Base Station.

Base Station: This is the central node in the network that receives the encrypted data from the sensor nodes. The Base Station stores the encrypted data and provides access to authorized users based on their attributes.

The Key Distribution Centre (KDC) is in charge of creating and providing the users with the cryptographic keys. A Master Key (MK) is created by the KDC and given to the Base Station. For each user, the KDC also produces a set of Secret Keys (SK) depending on their characteristics.

Users: The users in the network are the military personnel who need to access the encrypted data. The users are authenticated by the KDC and provided with the appropriate Secret Key based on their attributes.

Implementation:

The following steps can be used to implement the suggested design for safe data retrieval in military networks using the CP-ABE algorithm:

Step 1: Create the keys

Based on each user's qualities, the KDC generates a Master Key (MK) and a set of Secret Keys (SK). Data is encrypted using the MK by the base station, and decrypted using the SK by the consumers.

Secondly, encryption

Utilising the CP-ABE technique, the sensor nodes encrypt the data acquired and send it to the base station. Based on the characteristics of the people who have permission to access the data, the access policy for the encrypted data is established.

Third Step: Data Storage

The base station keeps the secured data

Third Step: Data Storage

Each data item's access policy and encrypted data are both stored in the base station's database.

Authentication and Authorization in Step 4

The KDC authenticates the user when they ask to view a data item. The KDC verifies the user's qualities before giving them the proper Secret Key (SK). If the user's attributes meet the access policy for the data item, the user can then use the SK to decrypt the encrypted data.

Fifth step: decryption

The user uses the SK that the KDC provides to decode the encrypted data. If the access policy for the data item meets the user's attributes, the user can then access the data.

Conclusion

In conclusion, safe data retrieval in military networks is crucial for preventing unauthorised access to critical data. It is essential to make sure that data is secured using strong encryption methods since wireless sensor networks (WSNs) are being used in military operations more and more. It has been demonstrated that the Cypher Policy Attribute-Based Encryption (CP-ABE) algorithm is a reliable method for protecting data in WSNs. The CP-ABE algorithm is a powerful technique for securing data in military networks using wireless sensor networks. The algorithm provides fine-grained access control, scalability, efficiency, and flexibility. It is a reliable and secure encryption technique that ensures privacy and confidentiality. However, there are still some challenges that need to be addressed, such as key management and device constraints. With further research and development, the CP-ABE algorithm can be improved to provide even better security and efficiency in military networks.

DOI : https://doi.org/10.56452/6-20

References

[1] S. K. Pandey, P. K. Jana, and P. K. Sahu, "Secure data retrieval in wireless sensor network using CP-ABE," in Proc. 2010 Int. Conf. Signal Proc. Commun. Comput. (ICSPCC), pp. 1–4.

[2] M. Liu, Z. Zeng, and S. Jiang, "Secure data retrieval scheme based on CP-ABE in WSNs," in Proc. 2011 IEEE Int. Conf. Internet Things (iThings), pp. 321–324.

[3] M. M. Hassan, A. Biswas, and M. A. Razzaque, "A secure data retrieval scheme for wireless sensor network using CP-ABE," in Proc. 2012 IEEE Int. Conf. Commun. Netw. (ICCNC), pp. 656–660.

[4] W. Zhang, C. Yang, and W. Su, "A secure data retrieval scheme for wireless sensor network using CP-ABE," in Proc. 2013 IEEE Int. Conf. Cyber Technol. Autom. Control (CYBER), pp. 53–56.

[5] H. Huang, S. Shao, and Y. Zhang, "A CP-ABE-based secure data retrieval scheme in wireless sensor networks," in Proc. 2014 Int. Conf. Comp. Network. Electron. Autom. (ICCNEA), pp. 153–156.

[6] W. Wang, J. Shao, and W. Zhang, "An efficient secure data retrieval scheme based on CP-ABE for wireless sensor networks," in Proc. 2015 IEEE Int. Conf. Cyber Technol. Control (CYBER), pp. 174–177.

[7] F. Yang, J. Li, and H. Li, "A secure data retrieval scheme based on CP-ABE and ECC for wireless sensor networks," in Proc. 2016 Int. Conf. Commun. Signal Process. (ICCSP), pp. 136–139.