



OPEN

Energy efficient trust aware secure routing algorithm with attribute based encryption for wireless sensor networks

M. Selvi¹✉, S. V. N. Santhosh Kumar², K. Thangaramya¹ & H. Abdul Gaffar¹

Attribute-Based Encryption (ABE) is one of the public-key cryptographic techniques which enforces a new method of security through effective control of access on the data which is stored or communicated in encrypted form using a variety of user defined access restrictions. ABE is implemented in a fully-fledged computer system, such as smartphones or embedded devices and it can be also used to enhance the security of network communication. In Attribute-Based Encryption, the encryption key will be associated with a set of attributes and these attributes are useful in the decryption process as well. Encrypting the data for numerous receivers can also be done with ABE, in such a way that only those with the right permissions can decrypt it later. The ABE provides a high level of security due to the wide range of key based qualities that can be defined, and it is also flexible enough to be used in a variety of communication and storage situations. In Wireless Sensor Networks (WSNs), the information is transmitted through wireless links from the sensors to a central location called the sink node. The nodes present in WSN are required to carry out the task of monitoring the environments, gather the necessary data through sensing, encrypt them and send them to the sink node. Therefore, security is a major concern for wireless communication since data is transmitted via an open wireless channel that can be accessed by malicious intruders. In order to handle the security problem, we propose a new Attribute-Based Encryption and Trust Based Secure Routing Algorithm (ABE-TBSRA) strategy by combining bilinear pairing and Diffie Hellman encryption scheme with RSA algorithm to encrypt and secure the data at the sender-side itself. In addition, we propose a new trust-based security model that uses three types of trusts namely direct, indirect, and historical trust values for improving the security. The major advantages of this proposed encryption and trust based secure routing algorithm include the enhancements in security level as well as packet delivery ratio, reliability of transaction and also the network throughput with reduced energy consumption and delay.

Keywords Wireless sensor network, Security, Attribute based encryption, Trust-based secure routing protocol, Diffie–Hellman with RSA and clustering method

Recent developments in Wireless Sensor Network (WSN) technology have made it possible to create optimal cost and power efficient power efficient design of sensor nodes with multiple functions. In wireless sensor networks, a huge number of resource-limited sensor devices are dispersed throughout the deployment region. Communication and cryptosystems both rely heavily on the security and confidentiality of the information they exchange. Though many different security methods are available for securing WSN in the provision of reliable data delivery, cryptographic techniques are the most efficient techniques as they can ensure confidentiality and data integrity effectively. In cryptography, encrypted data can be deciphered by using crypt analysis techniques when the keys are not known. There are two main methods of encrypting data namely the encryption based on symmetric keys and asymmetric keys¹. Symmetric key algorithms are easy to design and perform the implementation when it is compared to the public key algorithms due to the use of single key in this type of algorithm by the sender and the receiver. In public key algorithm, different keys are used by the sender and receiver and hence it is more complex with respect to design but provides enhanced security. Based on these requirements, we propose a new attribute-based encryption algorithm by extending the bilinear pairing and

¹School of Computer Science and Engineering, Vellore Institute of Technology, Vellore, India. ²School of Computer Science Engineering and Information Systems, Vellore Institute of Technology, Vellore, India. ✉email: Selvi.m@vit.ac.in

Diffie–Hellman encryption method with RSA algorithm for developing a new trust and encryption based secure routing protocol for secure delivery of data in WSNs.

In the past, many researchers developed encryption schemes for securing the data communicated through the network. Moreover, the Attribute Based Encryption (ABE) security technique can provide an authentication protocol for encrypted data by applying private keys to form cypher-text and by using access control policies on the required attributes². The authors in³ proposed an ABE that provides encryption as well as a fine-grained authentication mechanism. Key Policy with Attribute Based Encryption (KP-ABE) and Ciphertext creation Policy through Attribute Encryption (CP-ABE) are two types of attribute-based encryption methods that were used in³ to encrypt the data. The KP-ciphertext ABE and decryption key are bound to the access policy, while the CP-ABE ciphertext and decryption key are linked to attributes. In order to enhance the security through high level attribute operations and also by applying more flexible access control policies, many ABE schemes have been proposed in the past in the provision of secured communication which includes the use of access control list with ABE. Moreover, the type of possible attacks and the methods for prevention are also discussed with respect to the handling of sensitive information⁴. All of these methods that are available in the literature on security are also prone to security attacks due to the presence of malicious users.

In order to handle the problem of key leakage that is used in encryption and decryption, we propose a secured key exchange scheme through the application of a new bilinear group based Diffie–Hellman approach for key generation which is used with RSA algorithm for effective encryption of the data to be communicated. Moreover, we also propose a new trust-enabled secured routing scheme which is used to secure the WSN communication from the attacks of malicious users. In this model, we form clusters and select a Cluster Head (CH) for each cluster and we choose a set of trusted CHs for routing more securely. The major contribution of this model includes security enhancement through enhanced cryptographic techniques and trust measurements, energy efficiency through clustering and improvement in network performance based on secure routing. Through wireless sensor nodes provide protection against malicious attacks on the network by applying firewalls and authentication methods, the security challenges are still existing in WSN. In this way, we propose a new routing algorithm that applies clustering and trust measurement and decision-making model to form the secure routing algorithms in combination with data encryption. Here, improved route discovery and route maintenance techniques are proposed by considering the trust values so that it is possible to make the proposed clustered-based routing algorithm more efficient in WSNs. The proposed secure routing protocol has a unique ability to prevent malicious attacks because of its operations and maintenance policies which are reliance on trust evaluation. In the proposed cluster and trust base secure routing algorithm, routing is performed through cluster heads. Here, the route discovery process evaluates the trust values for selecting the next node for forwarding the data.

This trust-based secure routing model is using the broadcasting feature present in the proactive based routing protocols that is providing the secured and trusted neighbour node to assign as the next hop as it is followed in⁵. In the proposed security model, the system ensures trust between the sender and the receiver through message exchanges before they start the actual communication. In this way, the network is able to identify the genuine as well as malicious nodes and use that information to provide the secured routing process by selecting the paths through the trusted and active nodes.

In this work, we propose a new ABE-TBSRA scheme based on bilinear pairing and Diffie–Hellman encryption scheme with RSA algorithm in order to maintain the confidentiality of the data. Along with this method, we propose a trust management scheme for developing the secure routing process which is used to send the data from source to the Base Station (BS) more securely. Moreover, clustering technique is used for formation of clusters along with cluster head selection in WSN. In this research work, we compute the trust score of nodes and paths which are computed based on the encryption and decryption attempts by the nodes in order to improve the reliability of routing process in wireless sensor networks by adding better security and functionality. This proposed method is particularly successful at finding solutions to the security issues by compromising the integrity which are introduced by the attackers that appear when transmitting data. This proposed model uses attribute-based encryption based on bilinear pairing and Diffie–Hellman scheme with RSA algorithm and we introduce a new key management technique for finding more reliable and secure routes in wireless sensor networks. Furthermore, this work examines the use of direct, indirect, and overall values of the computed trust obtained through the proposed model for enhancing the security of WSN communication.

The main and important contributions of this proposed work are as follows:

- A new ABE-TBSRA has been proposed and implemented in this research work in order to reduce and optimize the energy consumption of the nodes and also the delay occurred in WSN communication.
- The proposed Attribute based encryption method uses the properties of bilinear pairing groups to secure the data communication by providing new key generation methods.
- For exchanging the keys between the sender and receiver, Diffie–Hellman encryption method with bilinear pairing scheme and RSA algorithm is used in the proposed algorithm ABE-TBSRA.
- The use of clustering of nodes in WSN and also performing the routing through CHs improves the network's resilience through reduction in hop count and also with respect to energy consumption in the routing process.
- A new trust management scheme has been proposed in this paper for providing improved security in the routing process for WSN communication.

Related works

There are numerous works which are present in the literature on security and secure routing algorithms^{6,7}. Since security is a major concern in WSNs, the proper handling of security is necessary either using encryption and decryption methods or using trust management techniques. The currently available data encryption

and decryption methods have either extremely high response times or extremely high computational costs, making them unsuitable for use in the securing of wireless sensor networks. In the past, various techniques were proposed to secure the communicated data with reliability to overcome the problems related to energy, coverage, security, and routing. A wide range of techniques are discussed in the literature for providing secure routing of data in WSN.

Han et al.⁸ propose an energy-aware and trust-based secure routing protocol for wireless sensor networks (WSNs) leveraging an adaptive genetic algorithm. The protocol optimizes routing by balancing energy efficiency and trustworthiness among nodes, ensuring secure and reliable data transmission. The adaptive genetic algorithm dynamically adjusts to network conditions, enhancing performance while extending the network's lifetime. This approach addresses key WSN challenges, including energy constraints, security risks, and maintaining consistent communication quality.

Aravindan and Rajaram⁹ present an energy-aware multi-attribute trust model designed for secure communication in MANET-IoT environments. The model evaluates nodes based on multiple attributes, such as energy efficiency and trustworthiness, to ensure reliable data transmission and robust security. By integrating energy-awareness into trust assessment, the approach extends network lifetime while mitigating risks from malicious nodes. This solution is tailored to address the unique challenges of MANET-IoT environments, including dynamic topology, resource constraints, and security threats.

Zhang et al.¹⁰ propose a secure routing strategy based on attribute-based trust access control for social-aware networks. The approach leverages attribute-based trust models to evaluate and select routing paths, ensuring that only trustworthy nodes are involved in data transmission. By incorporating social-awareness, the strategy accounts for the relationships and behaviors of nodes in the network, enhancing security and reliability. This method aims to mitigate security risks, such as attacks and data breaches, while optimizing routing efficiency and trust management in dynamic network environments.

Feroz Khan¹¹ presents an Enhanced Multi-Attribute Based Trusted Attack Resistance (EMBTR) model for secure routing of sensor nodes in WSNs. The model incorporates multiple attributes, such as energy levels, trustworthiness, and node behavior, to assess and select the most reliable routing paths. EMBTR enhances network security by identifying and resisting attacks while ensuring efficient communication. The approach is designed to handle the unique challenges of WSNs, such as resource constraints and vulnerability to malicious nodes, offering a robust solution for secure data transmission in these networks.

Khan and Rajalakshmi¹² propose a multi-attribute-based trusted routing approach for embedded devices in MANET-IoT environments. The model evaluates various attributes, such as energy, trust, and connectivity, to ensure the selection of reliable and efficient routing paths. By integrating trust management with multi-attribute analysis, the approach enhances the security and performance of communication in dynamic, resource-constrained networks. This method addresses key challenges in MANET-IoT systems, including node mobility, limited resources, and the need for robust data transmission, providing a secure and efficient solution for embedded devices.

Yesodha et al.¹³ introduce an elliptic curve encryption-based energy-efficient secured Ant Colony Optimization (ACO) routing protocol for WSNs. The protocol combines the advantages of elliptic curve encryption for data security with the energy-efficient capabilities of ACO to optimize routing paths. It ensures secure data transmission while minimizing energy consumption, addressing the challenges of energy constraints and security in WSNs. This approach enhances network lifetime, improves security, and ensures reliable communication in dynamic and resource-limited environments like WSNs.

Rani et al.¹⁴ provide a comprehensive survey on attribute-based encryption schemes for next-generation wireless IoT networks. The paper explores various encryption techniques that enable fine-grained access control, where data access is determined by specific attributes or characteristics of the user. These schemes offer enhanced security for IoT networks by ensuring that only authorized users with the correct attributes can access sensitive information. The survey also examines the challenges and potential solutions in implementing attribute-based encryption in dynamic and large-scale IoT environments, focusing on scalability, efficiency, and privacy.

Dinesh and Santhosh Kumar¹⁵ propose an energy-efficient, trust-aware, and secure neuro-fuzzy clustering technique for wireless sensor networks (WSNs) using sparrow search optimization. The approach combines the benefits of neuro-fuzzy systems for clustering with sparrow search optimization to enhance energy efficiency and security. It incorporates trust management to ensure secure data transmission while minimizing energy consumption. The proposed method aims to optimize network performance by balancing clustering accuracy, energy efficiency, and trustworthiness, making it well-suited for resource-constrained WSNs.

Diarra and Islam¹⁶ introduce an energy- and trust-aware routing approach for wireless networks to optimize multimedia data transmission. By selecting nodes with higher energy and trust levels, the model reduces energy consumption, enhances security, and ensures reliable data delivery. This approach improves the quality of service (QoS) for multimedia applications by addressing challenges like bandwidth demands, data integrity, and latency.

In¹⁷, the authors proposed an attribute-based encryption technique, and they send the encrypted data using this advance cryptosystem, since it supports the key establishment values, and it also increases the productivity of key concerns in the formation of ciphertexts. Jie Ling et al.¹⁸ proposed a multi-authority and attribute-based encryption scheme that is having traceable as well as dynamic updating policies by using finite groups to handle the domain attributes, expressive power and finally security in WSN.

In¹⁹, the authors proposed a new method for securing the data communicated through the network and stored in a repository that can be used for private data retrieval based on the cypher text policy of attribute-based encryption techniques proposed by them. In their model, the trust values are evaluated across all the nodes of the network, and it is updated in the trust table on a regular basis. From the experiments carried out by them, the authors have proved that their model significantly improved the performance of the network by reducing the communication cost. According to the authors, the use of trust mechanisms and encryption policies with

intelligent agents was a limitation of their research work. Shi et al.²⁰ proposed a new ABE encryption scheme for handling the security issues by encrypting the plain text by applying their scheme since it provides a structured method in storage of data and hence must be encrypted with similar structure. They applied their algorithm and compared it with Chinese remainder theorem-based encryption method. In²¹, the authors have provided a detailed review on the use of attribute-based encryption in cloud databases for secure storage. They proved that their method provided security in searching and storing the information in the cloud database more efficiently. In²², the authors proposed a new key distribution model using Elliptic Curve and Diffie–Hellman based key exchange mechanism that allows the sending user to satisfy the required security mechanisms. In their model, they improved the security and reduced the energy consumption. Kwon et al.²³ have proposed a novel Device to Device (D2D) authentication mechanism which used the Ciphertext-Policy (CP) based encryption/decryption method for protecting the key generation process. The major advantages of their security model include the increase in reliability and security through cryptographic approach.

In²⁴, the authors proposed a new method for protecting the privacy of the CP-ABE scheme using the keyword-based searching techniques. According to the authors, their model is more suitable for use with limited resources and they provided the security using bilinear Diffie–Hellman expectation algorithm. Sabrina Sicari et al.²⁵ provided a critical analysis by comparing the existing CP-ABE with other sticky policy methods for improving the security of data in their application. In²⁶, the authors proposed a new encryption method based on ABE and they claimed that their method is resistant to traffic snooping, sensor concessions, and the use of unauthorised data access. They used a Merkle tree-based data structure for modelling the network. Mriganka and Mandal²⁷ proposed a ciphertext policy-attribute-based broadcast authentication scheme which provides full anonymity through the modification of an identity-based encryption structure over bilinear pairings for enhancing security in communication.

In²⁸, the authors have developed a new trust aware and low-energy based adaptive clustering protocol. Their protocol was able to enhance the energy performance and also it avoided the elevated node power consumption problem. The major uses include enhancement in security and network lifetime. In²⁹, the authors proposed a realistic and trust-aware, secured routing algorithm to detect and prevent the malicious nodes from participating in the communication process using a hybrid trust model. They performed a statistical analysis and carried out packet switching through multivariate regression analysis. In spite of the presence of many encryption schemes and trust mechanisms, the security strength of the existing algorithms is not able to maintain the necessary levels in sensitive WSN applications.

In³⁰, authors have proposed an efficient attribute based revocable encryption scheme which ensures data integrity during message transmission. Their scheme employs ABE which encrypts the data by using attributes to maintain integrity during message exchange and it can be revocable. The advantages of the scheme are it performs efficient encryption of messages and prevent the intruders to intercept the messages during the transmit. However, the limitations of the scheme are it suffers from overhead in terms of communication and computation.

In³¹, authors have proposed an efficient policy based multi-party attribute based encryption scheme to ensure efficient and secured cloud storage. In their scheme, they have formulated the policy for multiparty attributes to ensure efficient encryption of data during the storage and also in transmit in the cloud environment. The advantages of the scheme are providing an efficient security mechanism in the cloud environment. The limitations are key revocation is not addressed in their scheme.

In³², authors have proposed an efficient Cipher Text Policy based ABE scheme with shared decryption in cloud storage. In their scheme, the messages are encrypted and decrypted by using CP based ABE scheme. The main advantages of the scheme are efficient encryption and decryption of the messages with less computational time. However, the limitations are it is prone to various types of security attacks which are caused by the various intruders. In^{33–35}, authors have proposed an efficient multiparty based fine grain ABE scheme for ensuring efficient security during message transmit in the network. The main advantages of the scheme are providing efficient encryption and decryption process with better communication and computation overhead. However, their schemes are most likely to be prone from various types of security attacks.

Based on the analysis of the literature survey, most of the existing schemes does not provide trade-off between energy efficiency and security. In most of the schemes available in the literature, they only either focuses on energy optimization for the nodes of WSN or providing security to the nodes of WSN. The major research gap identified in the literature survey is most of security schemes suffers from high computation overhead and they are vulnerable to various types of attacks caused by the intruder. Moreover, due to the resource constraint nature of WSN, there is a high requirement of light weight trust based authentication schemes which are required to provide better security with optimized energy consumption. Therefore, we propose a more efficient ABE encryption scheme by extending the ABE schemes along with trust-based routing for enhancing the communication security.

Proposed methodology

In this paper, we have proposed an effective Attribute based Encryption scheme along with a Trust model for measuring the characteristics of nodes to develop the proposed secure route algorithm called ABE-TBSRA. This algorithm uses ABE for encryption, trust measurement for selecting secure nodes and finally we use bilinear pairing with Diffie–Hellman algorithm for key generation. Moreover, the keys are used in the RSA algorithm for enhancing of the communication security in WSN. Figure 1 gives the components of the proposed system which consists of the major modules namely data source, security module, clustering module, routing module, decision manager and knowledge base.

The functions of the system have been detailed in this section. Here, the data which are collected by the sensor nodes are first encrypted by applying the ABE approach. Moreover, clustering and CH selection are carried out

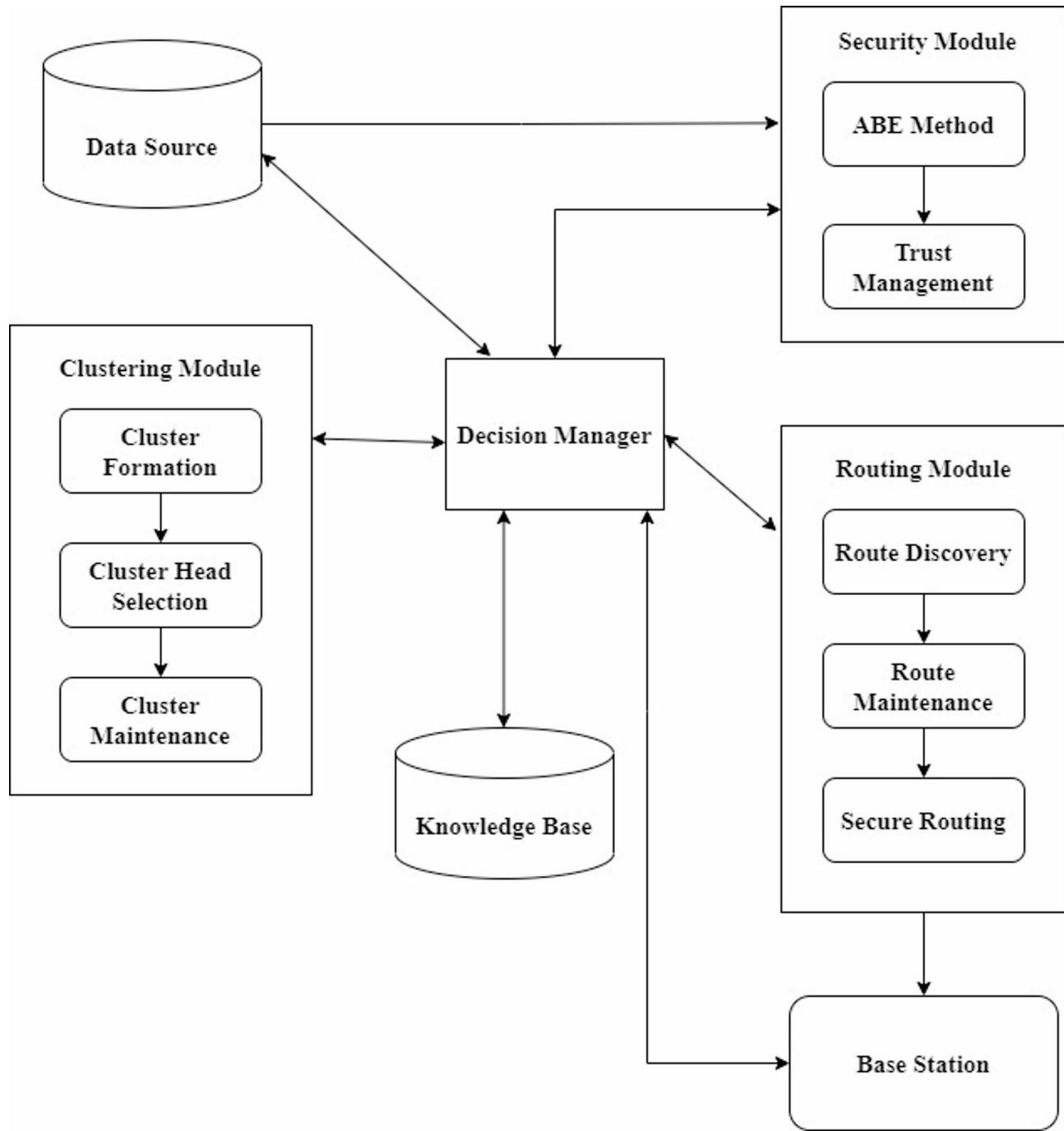


Fig. 1. System architecture.

for improving the energy efficiency. All the modules shown in this architecture are monitored and controlled by the decision manager. We use the security module to perform key generation and exchange, encryption/decryption and also trust measurement and management. There is a knowledge base in the system that provides the security rules and attacker related rules for monitoring the communication through inference. The routing module is coordinating with the other modules by the direction of the decision manager for secured delivery of data collected from the sensor nodes to the sink node as it is done in^{36,37} with suitable security enhancements.

Key generation

A generation of keys takes the authority of the system by using master keys with the set attributes are used as the input by the user and the secret key as the output in the encryption system. It is initially executed by the decision manager present in the base station of the wireless sensor networks by the use of a sub component namely the Key Generator Admin (KGA). Here, the KGA issues a set of secret keys initially that correspond to the attributes of each node. It assumes that the proposed model first sets-up the network initially and encrypts

the data to be communicated through the network using key generation method³⁸. In addition, the KGA makes public key parameter as pk and a master key parameter as mk . The KGA attains the necessary permissions from the database manager and then it confirms to the distribution of the keys more effectively with the cluster head nodes. Next, it generates a key to be used between two parties using the Diffie–Hellman encryption scheme with RSA algorithm and it is communicated through the network. In the key generation phase, two parties namely Alice and Bob who need to construct the transmission values of g and h which are to be prime numbers. The communication values are calculated by using this formula as $p = H \bmod G$, where p is the remainder obtained from $H \bmod G$ operation. Now, the two parties exchange control packets for purpose of knowing each other. In this work, new values are generated by using the formula and the keys are known by both parties are G and H , then the private key is generated by the decision manager and the secret keys are passed to both the parties with the help of security manager. Now, A chooses a value x and computes the value of p^x and B chooses the value of y and computes the value of p^y . now, A sends p^x to B and B sends p^y to A. A and B compute the values of $c = (p^y)^x$ and $d = (p^x)^y$. Since both are producing the same value, they are verifying the values of c and d for validating their keys. These keys are used along with RSA algorithm for effective encryption of the first attribute. This procedure is repeated for all the attributes by considering a set of x values namely x_1, x_2, \dots, x_n and set of y values namely y_1, y_2, \dots, y_n for encrypting n given attributes. The verification process is based on the values of c with c_1, c_2, \dots, c_n and d with d_1, d_2, \dots, d_n . If the values are matching the RSA based encryption is performed by the respective keys of A and B for encrypting their attributes before performing the communication.

Key distribution, encryption and decryption

The key distribution technique provides a user A with an encryption key $ek(x)$ and the receiving user B with a decryption key called $dk(x)$. If the new user joins the group and then the old user decides to get a new decryption key because the existing key has been expired or it has been negotiated. In this model, a trusted third party is present in the base station of the network for performing key generation and key distribution more effectively. Moreover, the trusted third party first defines the access policy for the sender A by generating new user key called x . The trusted third party of the proposed system is responsible for applying the access policy of the application for generating the required keys for encryption and decryption and then by assigning them to each user. Once the trusted third party has well-defined the users access control policy p^x , it creates the sender's encryption key $ek(x)$ and forms the decryption key $dk(y)$ by executing the following equation.

$$ek(x) = KG(p^x, p^y, \phi(xy), d, e) \quad (1)$$

$$dk(y) = KG(p^x, p^y, d, e) \quad (2)$$

where KG is the key generation function used for all the nodes in the cluster formed in this work from the nodes of the WSN. The trusted third party encrypts the message using the equation.

$$CT = Enc(PT, ek(x)) \quad (3)$$

Here CT is the cipher text, $\phi(x)$ is the Euler's phi function and PT is the plain text. Moreover, the encryption process calls the RSA algorithm with Euler's phi function. The message is sent from the sender side to the receiver's side namely the base station in encrypted form. The received message is decrypted at the base station using the equation.

$$PT = Dec(CT, dk(y)) \quad (4)$$

Here, the verification of the users is performed using Diffie–Hellman key exchange method with RSA algorithm along with access policy of the application with the support of the trusted third-party present in the base station.

Trust computation

The trust values are combined into the cluster heads for selection process. The trust value of a nodes in a cluster is taken into account by the CHs nodes in the present round at secure routing process. Nodes with a high degree of trust are more likely to be chosen as path discovery transmission relays³⁹. Trust values consist of three parts namely direct, indirect and overall trust values.

Direct trust value

In this work, a direct trust model computes every cluster in its own value called Direct Trust (DT) computation is based on the composed and direct packages to its neighbours⁴⁰, which allows it to calculate its implication with each neighbour and current DT of node a, then the actual degree of trust with respect to its neighbor b node, which is given by equation.

$$DT_{ab}^n = \alpha * (\beta_1 rcvd_p + \beta_2 snd_p)^{n-1} + (1 - \alpha) * (rcvd_p + snd_p)^n \quad (5)$$

Here, DT_{ab}^n stands for direct trust value of node n obtained by sending the message from the user a to user b. the values of this value are more important for effective decision making. In the former scenario historical trust value, it denotes the trustworthiness in the past⁴¹, whereas the later current trust value means that reliability now.

$$rcvd_p = \frac{\text{receive_message}_b}{\text{message}_b} \quad (6)$$

α and $(1 - \alpha)$ ($0 < \alpha < 1$) are the weights that correspond to history and current trust values and it can vary with individual uses of WSNs. Finally, $rcvd_p$ and snd_p are the ratio of sent and received packets over total packets⁴² which is represented as

$$snd_p = \frac{send_message_b}{message_b} \quad (7)$$

Additionally, volatility or uniqueness factor β_1 and β_2 have been established to expeditiously filter out malevolent nodes, which were once normal sensor nodes were increase their trust levels. In order to return a previous trust level to a normal range⁴³, the formulas shown in equation.

$$\beta_1 = e^{-f_1 \bmod (T, \lambda)} \quad (8)$$

$$\beta_2 = e^{-f_2 \bmod (T, \lambda)} \quad (9)$$

where T is the present time of the system and λ is the time threshold. Next, the f_1 and f_2 are factors used to regulate the rate of change in trust value. In order to avoid miscategorized valid nodes, like those that have been off of the network in distribution and forwarding packets for a long time are mod (T, λ), the training part is strengthened with trust management. To keep track of the past trust values which are becoming too tiny or to make sure that volatile factors degrade over time in a particular range, the proposed algorithm uses temporal rules. Moreover, the values of λ , f_1 and f_2 are application-specific.

Indirect trust value

The third-party network node trust relationship is utilised in the computation of Indirect Trust (IT) values for nodes a and b. The node s_a has a reputable status because it belongs to a third party. Node a is a trusted assessor, node b is for calculating the target and node s_a is the recommended of sensor node a. Here, $s_a \in s_p = \{s_1, s_2, \dots, s_c\}$, where c is the common trusted nodes and s_p is the set of public trusted neighbor nodes of node a and b. The IT value of node a to node b is shown in⁴⁴ based on the relationship given in equation.

$$IT_{ab}^n = \frac{1}{c} \sum_{s_a \in s_p} (DT_{a*s_a}^n * DT_{s_a*b}^n) \quad (10)$$

where $DT_{a*s_a}^n$ is the direct trust value of node x to s_a and $DT_{s_a*b}^n$ is the DT of node s_a to b, where node s_a is any public trusted neighbor of a and b. Node s_a will be removed from the set of public trusted neighbors if the trust value of node a to s_a is less than threshold.

Overall trust value

The Overall Trust (OT) values are computed the overall performance of direct and indirect values with their weight factors. The nodes are communicated with a third-party trust management scheme. Finally, the nodes are transmitted the data through the trust factors with more reliable and secure in their routing process⁴⁵. Finally, the overall trust value is computed using the formula:

$$OT = ((w1 * DT) + (w2 * (\beta_1 + \beta_2)) + (w3 * IT) + (w4 * \alpha))/4 \quad (11)$$

In this work, the value of OT must be greater than or equal to 0.65 for a node to be recognized as a genuine node for communication.

Clustering and cluster head selection

The routing performance in wireless sensor networks can be extended by using clustering techniques. In this work, we propose a cluster-based routing algorithm and hence it has a mechanism for selecting the CH in each round. Since, it takes more energy to re-cluster, clustering often will reduce the network's life expectancy^{46,47}. Therefore, this work performs CH rotation only after the energy level and trust level of the CH goes below a threshold value. In this model, clustering is accomplished by dividing the network into a number of unequal groups and hence the clustering process is validated using rules. Using the proposed clustering and cluster-based secure routing algorithm, the CHs are selected for each of the clusters from the cluster members node with minimum distance, high energy, low mobility and also with trust values⁴⁸. When two or more nodes have the same transmission power, the nearest node to the cluster's centre is selected as the new CH. The CH selection and rotation are carried out in this work using a mathematical model based on the computation of a threshold value, THV(a). Cluster members of a cluster will decide on whether a new CH is needed for the current round based on the current threshold value during every round of the cluster-based routing process⁴⁹. If a new node has the possibility of becoming a cluster member in a cluster working under a CH, it can choose its own cluster from the nearest clusters based on distance. In order to support in decision-making, each new node is assigned a trust value between 0 and 1. If the value is greater than the variable THV(a) in the equation, then the current node will become a possible candidate node for inclusion in the next round. The value of THV(a) for a node a is computed using the formula

$$THV(a) = \left\{ \frac{P}{1 - P * (r \bmod \frac{1}{P})} \right\} \text{ if } a \in s \quad (12)$$

where s represents the set of sensor nodes that did not change from CH to non-CH in the preceding round with the value $1/P$. Here in round r , the percentage of CHs in a network is considered as P , n is the total number of nodes, and r is the present round. The function, $\text{Mod}()$ returns the remainder after a number is divided by the divisor, which ensures the nodes with equal opportunity to become the CH.

Cluster and trust based secure routing algorithm with energy efficiency

In this work, we proposed a novel ABE-TBSRA attribute-based encryption strategy by combining bilinear pairing and Diffie Hellman and RSA based encryption scheme to encrypt and secure the data. This algorithm provides a method for calculating the key management for encrypting and decrypting the data with most secure, and quickest way to transfer the data packets from the source to the destination. This protocol is an optimized routing protocol in which the nodes are clustered and it provides an optimal path for effective routing in WSNs. In this section, we have given a complete description about our proposed ABE-TBSRA method. In this model, bilinear mapping is used to construct the keys using Diffie–Hellman key exchange with RSA algorithm. Moreover, we consider two cyclic groups namely G and G_m to form the bilinear pairing. The main advantage of using bilinear pairing along with Diffie–Hellman algorithm with RSA algorithm is to enhance the security by making use of the difficulty present in the discrete logarithm problem.

In this model, the trusted third-party present in the base station is responsible for selecting the groups G and G_m along with the generator g for the cyclic groups. This value of g is used to compute the values of g^x by the sender and g^y by the receiver. Key sharing is accomplished by the combination of bilinear pairing with Diffie–Hellman algorithm. In this proposed ABE scheme, separate keys are computed for each of the attributes namely a_1, a_2, \dots, a_n . For each attribute the sender is selecting a prime number x and hence the sender selects a set of prime numbers namely x_1, x_2, \dots, x_n and the receiver also selects a set of prime numbers y_1, y_2, \dots, y_n . These values are used for generating the keys for encryption and decryption using RSA algorithm and they are also used for key verification and user authentication by applying bilinear Diffie–Hellman scheme with RSA algorithm. The algorithm for our proposed ABE-TBSRA method are as follows.

Input: PT message, generator value g , attribute keys x from the sender and y from the receiver.

Output: Packets encrypted to get CT and delivered at destination.

Step-1: Request the key distribution sender to authenticate the sender Alice (A) and the receiver Bob (B) by sending the credentials of A and B using the format $ID_A \parallel \text{IP-ADDR}_A \parallel \text{PWD}_A$ and $ID_B \parallel \text{IP-ADDR}_B \parallel \text{PWD}_B$.

Step-2: If A and B are authenticated successfully, the trusted third party creates groups G and G_m to form a bilinear pairing and gets the prime number g which was used as the generator of the cyclic groups G and G_m .

Step-3: For generating the encryption and decryption keys, the trusted third party chooses a large prime number p from the two groups namely G and G_m using the formula $p = G_m \bmod G$.

Step-4: A chooses a value of x and computes the value p^x and B chooses the value of y and computes the value p^y .

Step-5: Now, A sends p^x to B and B sends p^y to A.

Step-6: A and B compute the values of $c = (p^y)^x$ and $d = (p^x)^y$.

Step-7: When A and B both are producing the same value, they are verifying the values of c and d for validating their keys. This way both parties are exchanging their keys with the help of trusted third party using bilinear Diffie-Hellman algorithm.

Step-8: Choose the nearest prime numbers to p^x and p^y to compute the encryption key $ek(x)$ and decryption key $dk(y)$ using the formula $ek(x) = KG(p^x, p^y, \phi(xy), d, e)$ and $dk(y) = KG(p^x, p^y, d, e)$

Step-9: The trusted third party encrypts the message using the equation $CT = Enc(PT, ek(x))$ by applying the RSA algorithm.

Step-10: Compute the overall trust values for each node i using the formula $OT(i) = ((w1 * DT(i)) + (w2 * (\beta_1 + \beta_2)) + (w3 * IT(i)) + (w4 * \alpha)) / 4$, where i varies from 1 to n .

Step-11: If the overall trust value is greater than 0.65 for the sender is allowed to send the encrypted data to the receiver through the intermediate CHs having a trust value of 0.65 or more.

Step-12: The received message is decrypted at the base station using the equation $PT = Dec(CT, dk(y))$

Step-13: Form the eligible nodes for the next round using the formula

$$THV(a) = \left\{ \begin{array}{l} P \\ 1 - P * (r \bmod \frac{1}{P}) \end{array} \right\} \text{if } a \in s$$

Step-14: Repeat the process until all the attributes are encrypted and sent through the eligible CH nodes.

Algorithm 1. ABE-TBSRA AlgorithmSecurity analysis

Formal security analysis plays a crucial role in ensuring secure data communication within WSN by rigorously evaluating the security properties and protocols involved. This involves using mathematical frameworks to validate confidentiality, integrity, authentication, and availability of data transmitted across the network. Security properties such as non-repudiation are formalized to ensure that entities involved in data communication cannot deny their actions. Moreover, access control mechanisms are verified using formal models to ensure that only authorized nodes can access sensitive data during routing and aggregation processes.

The analysis also assesses the robustness of data communication protocols against threats like insider attacks, Sybil attacks, and replay attacks. By leveraging formal methods, researchers can establish a mathematically sound foundation for security claims, offering higher assurance against vulnerabilities. Such analysis forms the cornerstone for designing secure and efficient routing protocols in WSNs, especially in applications requiring stringent data confidentiality and integrity.

In the proposed secure data communication approach, efficient encryption techniques are employed to safeguard routing in WSNs. The columnar transposition cipher method is used to establish secure communication between sensor nodes and their cluster head nodes, while the Residue Number System (RNS+) technique enhances security in communications between CH nodes. The security analysis focuses on two key aspects: correctness and confidentiality. Correctness ensures that the sink node accurately receives the data after applying encryption techniques, while confidentiality prevents unauthorized access to sensitive information during routing.

Theorem 1 The proposed secure communication method ensures that the sink node receives data accurately after encryption.

Proof The proof is based on an attack model where attackers are limited to eavesdropping on communication channels without the ability to modify or replace messages. The encryption algorithm ensures that CH nodes encrypt data using a cryptographic key before transmission. The CH node decrypts these encrypted messages to retrieve data from its associated nodes. Since the cluster key is exclusively shared among legitimate nodes within the cluster, it remains inaccessible to unauthorized entities. This secure key-sharing mechanism guarantees the correctness of data communication within the cluster.

Theorem 2 The proposed method ensures the confidentiality of data during communication.

Proof During data communication and aggregation within a cluster, encryption renders the content inaccessible to attackers without the cryptographic key. Additionally, obtaining unique parameters such as sensor node IDs, hash messages, and encrypted cryptographic keys is infeasible for attackers. These parameters are exclusively known to the base station and the respective CL nodes, adding another layer of security. The use of diverse, node-specific parameters ensures robust confidentiality.

Furthermore, the proposed method is resilient to eavesdropping, traffic analysis, and node capture attacks. Encrypted data and secure key management mechanisms make it challenging for attackers to extract meaningful information, ensuring secure and efficient routing in WSNs.

Informal security analysis

The informal security analysis demonstrates that the proposed system effectively counters a variety of threats, including Sybil, replay, eavesdropping, and node capture attacks, while maintaining data confidentiality, integrity, and authenticity. By combining efficient encryption techniques, secure communication protocols, and proactive defence mechanisms, the system ensures reliable and secure data communication in WSN routing. An informal security analysis for the proposed system would focus on evaluating the system's ability to resist common security threats in a practical and conceptual manner, without relying on formal proofs or mathematical models.

Resilience against Sybil attacks

The system employs robust authentication and validation mechanisms to verify the legitimacy of each node participating in the network. By using secure key management, digital signatures, and reputation systems, it ensures that malicious nodes cannot create multiple fake identities to disrupt the network. Additionally, anomaly detection algorithms actively monitor the data for irregular patterns, effectively identifying and mitigating Sybil attacks. These features bolster the system's ability to maintain trustworthiness and integrity in routing operations.

Prevention of replay attacks

The system incorporates timestamping and nonce values to verify the freshness of each message. This ensures that repeated or outdated data is automatically discarded. Furthermore, the use of secure authentication mechanisms guarantees that only legitimate nodes can send or receive data. Since the system authenticates every message entering the network, it effectively blocks replay attempts and maintains the integrity of the routing process. This makes the system particularly resilient to time-based attacks where attackers attempt to reuse valid data packets.

Protection against eavesdropping attacks

To guard against unauthorized interception, the system employs strong RSA encryption technique. These encryption methods ensure that even if communication is intercepted, the data remains unintelligible to attackers. Additionally, the secure communication channels used between nodes and clusters further enhance data confidentiality. This proactive approach ensures that sensitive information, such as routing paths or sensor data, remains protected from prying eyes, preserving privacy.

Defence against node capture attacks

Node capture attacks pose a significant threat in WSNs, as attackers can compromise nodes to extract sensitive keys or disrupt network communication. The system mitigates this threat by limiting the exposure of cryptographic keys. Only legitimate cluster nodes and the base station have access to the necessary encryption parameters, ensuring that even if a node is compromised, the overall network security remains intact. The system's hierarchical design minimizes the impact of such attacks by isolating compromised nodes and maintaining secure communication among unaffected nodes.

Secure routing and data integrity

The system ensures secure routing by implementing encryption at multiple levels. Sensor nodes encrypt data before sending it to the cluster head, and further encryption is applied during inter-cluster communication. The hierarchical use of encryption prevents unauthorized modifications to the data while ensuring that the base station receives accurate and reliable information. This approach also guards against data tampering during transmission, preserving the integrity of routing and aggregation processes.

Mitigation of insider threats

Insider threats, where malicious nodes within the network attempt to disrupt operations, are addressed through efficient authentication and authorization mechanisms. Only nodes with valid credentials can participate in the network, and the distributed nature of the system ensures that malicious nodes are quickly identified and isolated. The system's anomaly detection further reinforces its defences by flagging suspicious activity from internal nodes.

Handling traffic analysis

To mitigate traffic analysis attacks, the system encrypts not only the data but also key routing information. This obfuscation prevents attackers from analysing communication patterns to infer sensitive details, such as node locations or the frequency of data transmission. By employing secure communication protocols, the system minimizes the risk of information leakage through traffic analysis.

Results and discussions

In this paper, a proposed ABE-TBSRA method has been simulated by using NS-2 simulator. Table 1 shows the parameters that are used for simulation of the secure routing experiments in WSNs carried out in this work. The experiments have been conducted in this work, the proposed method is evaluated and its performance is compared with existing algorithms are CKM-ABE⁸, LEACH-TM¹⁹ and TASRP²⁰.

Security level with encryption

The proposed ABE-TBSRA algorithm has been implemented and has been evaluated by comparing with three existing protocols namely CKM-ABE⁸, LEACH-TM¹⁹ and TASRP²⁰. The evaluation has been carried out with several numbers of attributes such as 10, 20, 30, 40 and 50. The security level comparison of the proposed algorithm and the existing algorithms are shown in Fig. 2.

From this Fig. 2, it is observed that the proposed algorithm namely ABE-TBSRA is higher in their security level with encryption techniques, when it is compared with other existing protocols namely CKM-ABE⁸, LEACH-TM¹⁹ and TASRP²⁰. The improvement in security level is obtained in this work by choosing keys with bilinear pairing, taking large prime numbers based on p^x and p^y values, use of trusted third party for key generation, key exchange using bilinear paired Diffie–Hellman algorithm and RSA based encryption before routing. Moreover, trust management is also performed in this work for improving the secure routing further. Figure 3 presents the proposed system's security level in comparison with the trusted nodes.

Packet delivery ratio

Packet delivery ratio analysis are shown in Fig. 4. Here, the proposed ABE-TBSRA algorithm has been related with the three existing protocols namely CKM-ABE⁸, LEACH-TM¹⁹ and TASRP²⁰. The experiments have been carried out with several numbers of sensor nodes such as 100, 200, 300, 400 and 500. Figure 5 presents the proposed system's packet delivery ratio in comparison with the trusted nodes.

From Fig. 4, it is perceived that the packet delivery ratio of the proposed ABE-TBSRA is higher than the existing protocols namely CKM-ABE⁸, LEACH-TM¹⁹ and TASRP²⁰. In this work, the packet delivery ratio is increased by performing suitable clustering and re-clustering periodically and also by rotating the cluster heads. Moreover, the trust management method proposed in this work enabled the detection of packet dropping attacks and hence the packet delivery ratio has been improved.

Parameters	Value
Network area	200 m × 200 m
Number of sensor nodes	100–1000
Basic routing protocol	LEACH
Initial energy oof nodes	2Joules
Mobility model	Random way point mobility

Table 1. Simulation parameters.

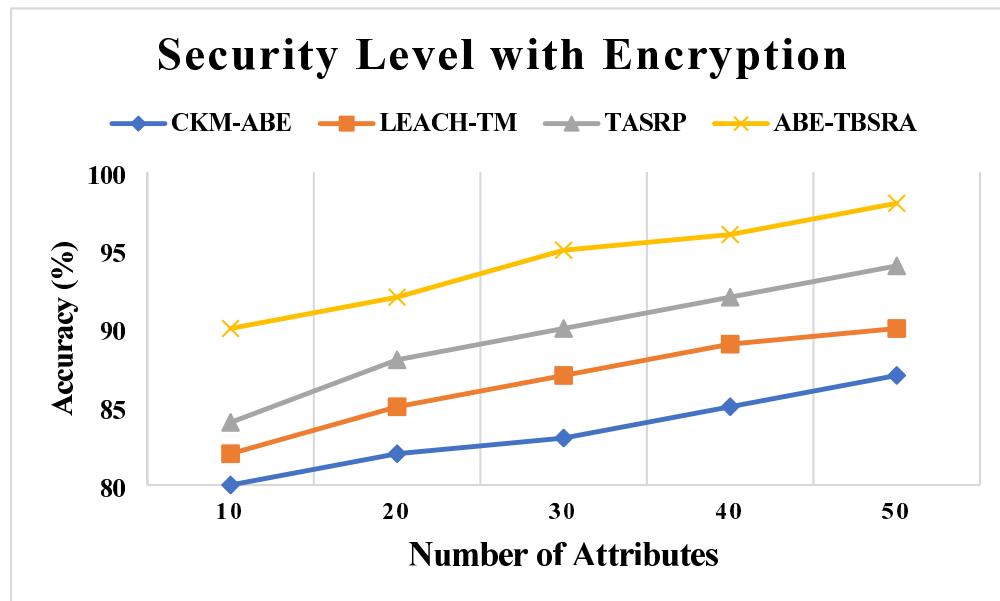


Fig. 2. Security level with encryption.

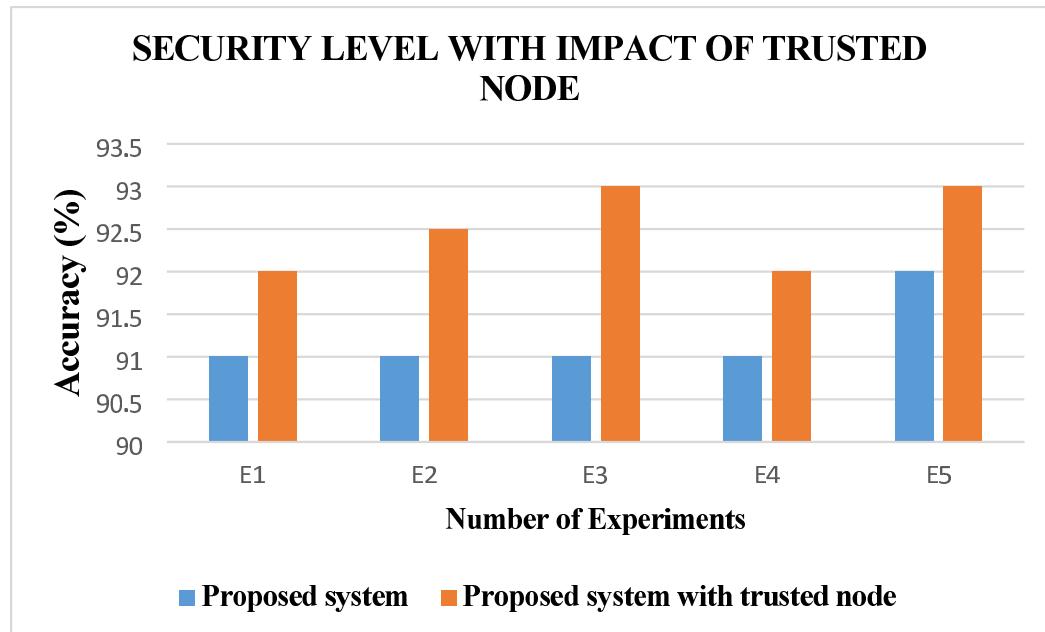


Fig. 3. Security Level with impact of trusted nodes.

Analysis of delay

The proposed ABE-TBSRA algorithm has been evaluated by conducting the experiments on the delay analysis by considering the values of delay between the ABE-TBSRA method and compared with other protocols namely CKM-ABE⁸, LEACH-TM¹⁹ and TASRP²⁰. The experiments have been carried out with a greater number of sensor nodes such as 100, 200, 300, 400 and 500. The analysis of delay is shown in Fig. 6.

From this Fig. 6, it can be observed that the ABE-TBSRA algorithm has decreased the delay when it is compared with the other methods namely CKM-ABE⁸, LEACH-TM¹⁹ and TASRP²⁰. In addition, the proposed algorithm has been made secured routing using direct, indirect and overall trust values. The reliability of the communication was ensured through security, leading to better route selection and fast communication, leading to reduction in delay. Figure 7 presents the proposed system's network delay in comparison with the trusted nodes.

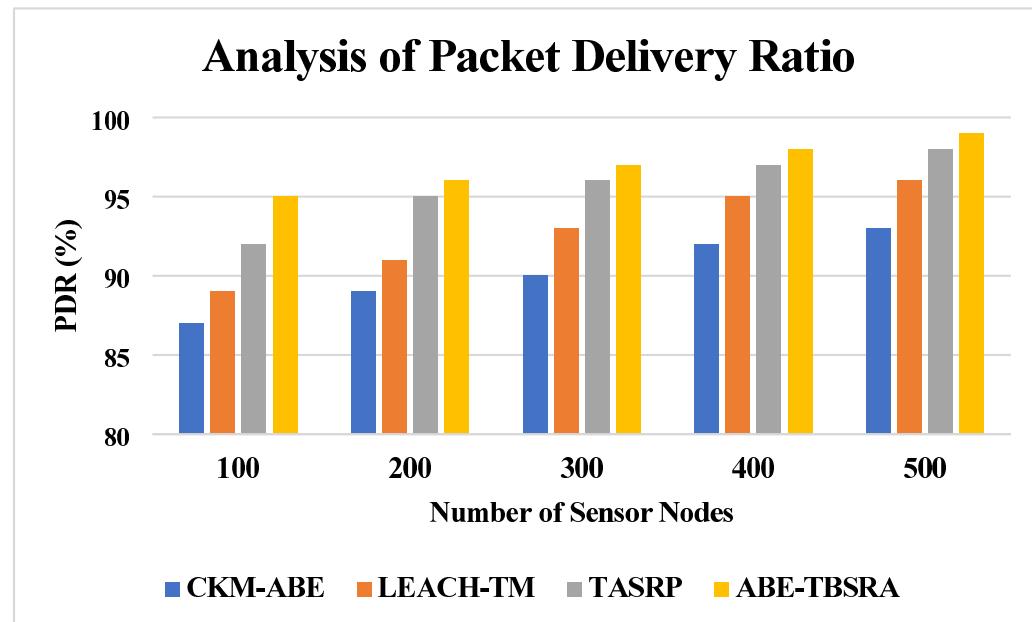


Fig. 4. Analysis of packet delivery ratio.

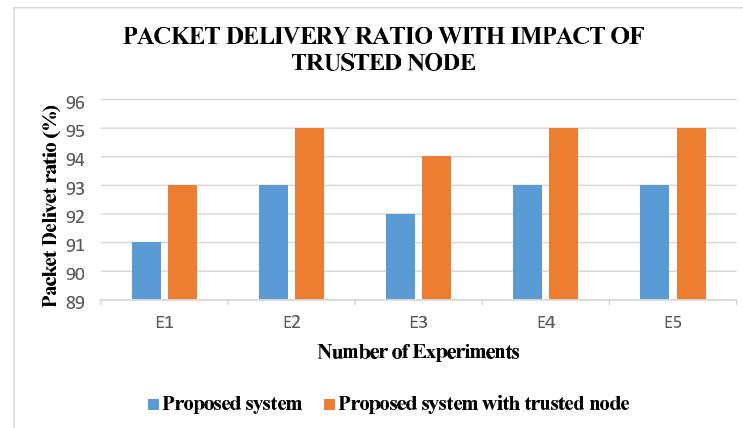


Fig. 5. Packet delivery ratio with impact of trusted nodes.

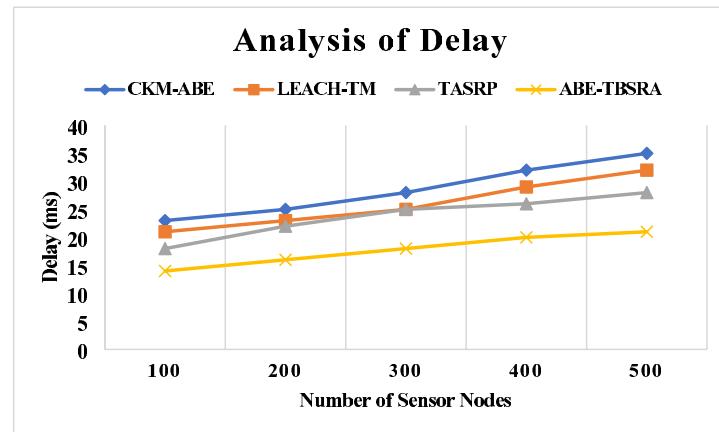


Fig. 6. Analysis of delay.

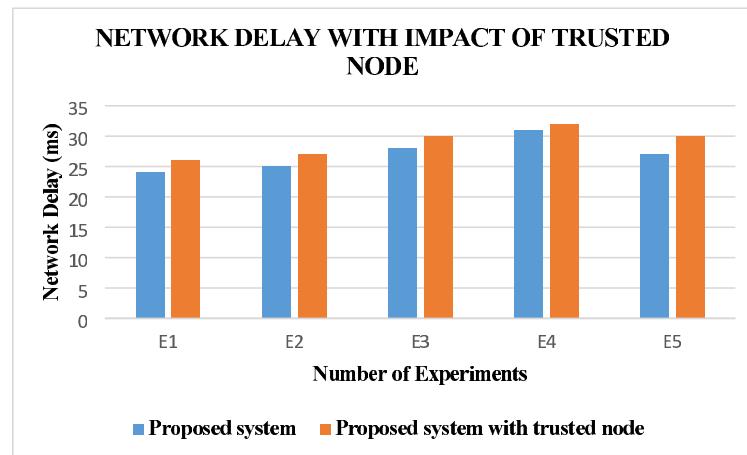


Fig. 7. Network delay with the impact of trusted nodes.

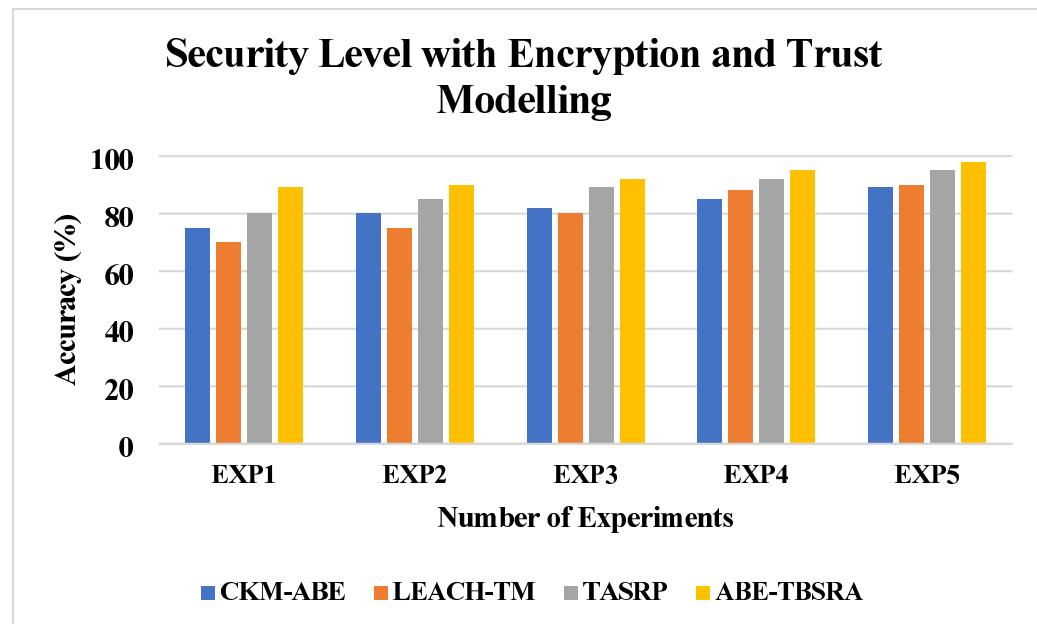


Fig. 8. Security level with encryption and trust modelling.

Security with encryption and trust modelling

The analysis of overall security with encryption and trust modelling is shown in Fig. 8. Here, the proposed ABE-TBSRA algorithm has been evaluated by conducting the experiments on the security with encryption of data packets before transmitting the packets and then improving the security further using trust-based secure routing method. Moreover, the proposed algorithm namely, ABE-TBSRA has been compared with other three existing protocols namely CKM-ABE⁸, LEACH-TM¹⁹ and TASRP²⁰.

From Fig. 8, it is observed that security level with encryption and trust modelling provides increased security when it is compared with the other methods namely CKM-ABE⁸, LEACH-TM¹⁹ and TASRP²⁰. The improvement is higher than only trust modelling because the copying of data packets is not useful to the malicious users since the data packets are sent in encrypted form. This leads to an increase in the type of passive attacks in addition to the reduction in active attacks through trust modelling.

Energy consumption

The results of the analysis obtained on the energy consumption metric is shown in Fig. 9. In this work, the proposed ABE-TBSRA algorithm has been evaluated by calculating and comparing the energy consumption of the proposed protocol for WSNs with the three existing protocols namely CKM-ABE⁸, LEACH-TM¹⁹ and TASRP²⁰. The experiments have been carried out with several numbers of sensor nodes such as 20, 40, 60, 80 and 100.

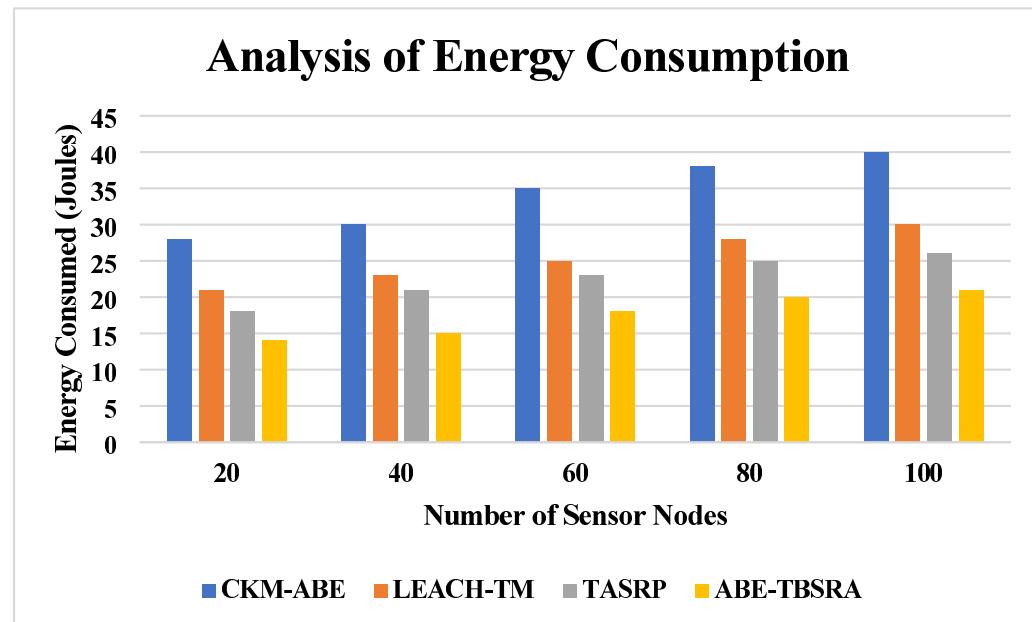


Fig. 9. Analysis of energy consumption.

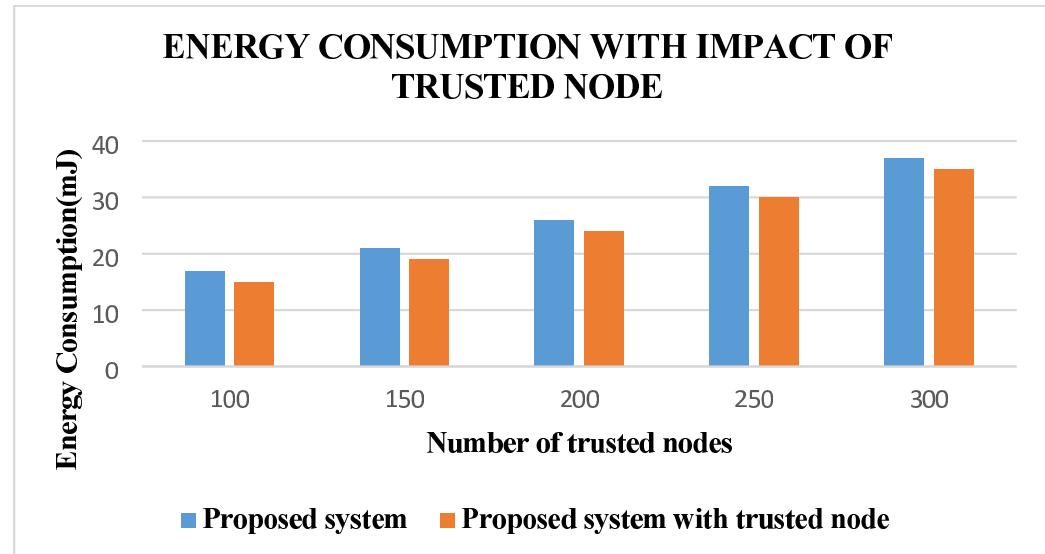


Fig. 10. Energy consumption with the impact of trusted nodes.

From this Fig. 9, it is observed that the energy consumption of the sensor nodes is decreased in the network along with the routing process using the proposed ABE-TBSRA than the existing protocols namely CKM-ABE⁸, LEACH-TM¹⁹ and TASRP²⁰. Moreover, the security model developed using ABE with bilinear and Diffie-Hellman and trust management for secure routing in the network enabled the reduction of energy consumption by preventing the attackers from reading the data packets communicated through the network. Figure 10 presents the energy consumption of the proposed system in comparison with the trusted nodes.

Overall network performance

The analysis of overall network performance is shown in Fig. 11. Here, the proposed ABE-TBSRA algorithm has been evaluated by conducting the experiments for analysing the overall performance of the network and by comparing the proposed algorithm with three existing protocols namely CKM-ABE⁸, LEACH-TM¹⁹ and TASRP²⁰.

From this Fig. 11, the overall network performance can be observed in the secure routing algorithm namely ABE-TBSRA developed using ABE and trust method shows the data transmission with high reliability by increasing the network lifetime and it is compared with the other protocols namely CKM-ABE⁸, LEACH-TM¹⁹

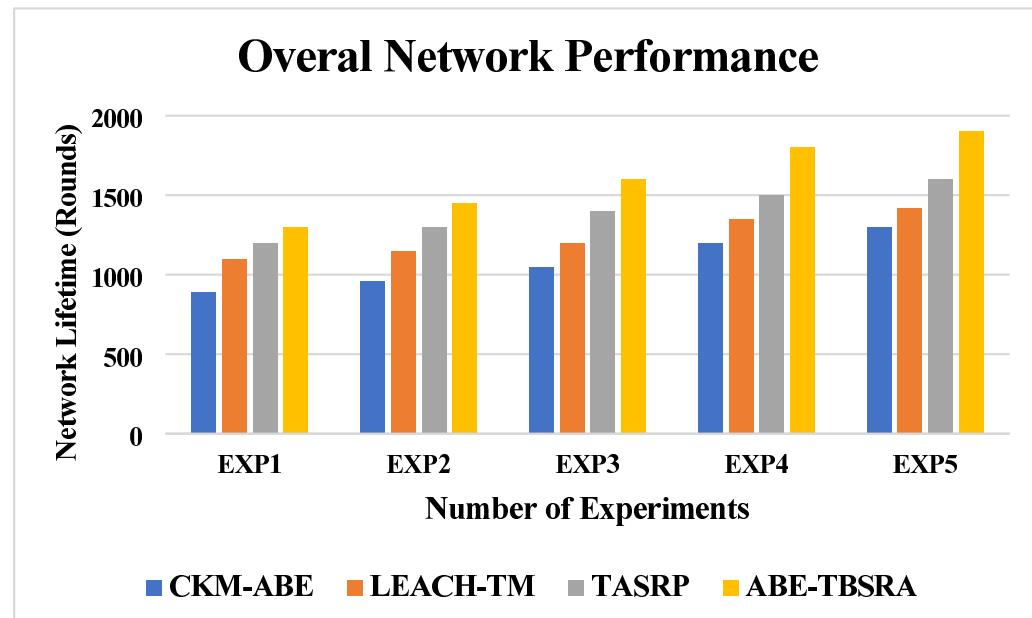


Fig. 11. Analysis of overall network performance.

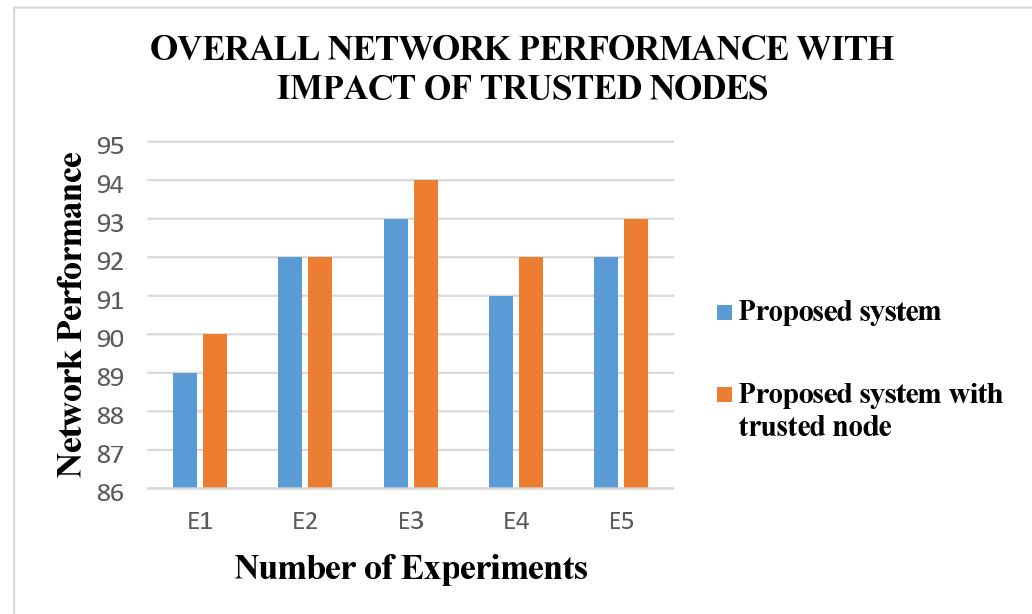


Fig. 12. Overall network performance with the impact of trusted nodes.

and TASRP²⁰. The proposed methods are enhanced due to the authentication, encryption, trust modelling, clustering, CHs, and secure routing process using security methods through the CHs. Figure 12 presents the overall network performance of the proposed system in comparison with the trusted nodes.

Conclusion

In this paper, a novel proposed algorithm called ABE-TBSRA along with clustering and security techniques to secure the data in an efficient method using WSNs. In this work, we used attribute-based encryption and key management to form the secure routing algorithm that uses clustering and cluster-based routing for reducing the power consumption. Moreover, it provided facilities for CH rotation after each round. A trust management scheme is also present in this work by using the results obtained from the bilinear pairing and Diffie–Hellman scheme along with direct trust, indirect trust and overall trust values. From these experiments, we observed that the security of the routing process is increased when it is compared with other existing secure routing protocols.

Future work, in this direction can be the inclusion of an intrusion detection system by exploring federated learning for improving the security. Moreover, block chain based light weight authentication protocols which can be further explored in providing better security with optimized energy consumption for the nodes of WSN.

Data availability

All data generated or analyzed during this study are included in this published article.

Received: 21 November 2024; Accepted: 21 May 2025

Published online: 05 June 2025

References

- Ali, S. et al. An efficient cryptographic technique using modified Diffie-Hellman in wireless sensor networks. *Int. J. Distrib. Sens. Netw.* **16**(6), 1550147720925772 (2020).
- Ali, M., Mohajeri, J., Sadeghi, M. R. & Liu, X. A fully distributed hierarchical attribute-based encryption scheme. *Theoret. Comput. Sci.* **815**, 25–46 (2020).
- Sahai, A., & Waters, B. (2005). Fuzzy identity-based encryption. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques* vol. 3494 457–473 (Springer).
- Han, D., Pan, N. & Li, K. C. A traceable and revocable ciphertext-policy attribute-based encryption scheme based on privacy protection. *IEEE Trans. Dependable Secure Comput.* **19**(1), 316–327 (2022).
- Bangotra, D. K., Singh, Y., Selwal, A., Kumar, N. & Singh, P. K. A trust based secure intelligent opportunistic routing protocol for wireless sensor networks. *Wirel. Pers. Commun.* **127**, 1045–1066 (2021).
- Muthurajkumar, S., Ganapathy, S., Vijayalakshmi, M. & Kannan, A. Secured temporal log management techniques for cloud. *Procedia Comput. Sci.* **46**, 589–595 (2015).
- Ahmed, A., Bakar, K. A., Channa, M. I., Haseeb, K. & Khan, A. W. A trust aware routing protocol for energy constrained wireless sensor network. *Telecommun. Syst.* **61**(1), 123–140 (2016).
- Han, Y., Hu, H. & Guo, Y. Energy-aware and trust-based secure routing protocol for wireless sensor networks using adaptive genetic algorithm. *IEEE Access* **10**, 11538–11550 (2022).
- Aravindan, S., & Rajaram, A. Energy-aware multi-attribute trust modal for secure MANET-IoT environment. *Multimed. Tools Appl.* 1–26.
- Zhang, X. et al. Secure routing strategy based on attribute-based trust access control in social-aware networks. *J. Signal Process. Syst.* 1–16 (2024).
- Feroz Khan, A. B. An enhanced multi attribute based trusted attack resistance (EMBTR) for the secure routing of sensor nodes in wireless sensor network. *Wirel. Pers. Commun.* **137**(4), 2397–2407 (2024).
- Khan, A. F. & Rajalakshmi, C. N. A multi-attribute based trusted routing for embedded devices in MANET-IoT. *Microprocess. Microsyst.* **89**, 104446 (2022).
- Yesodha, K., Krishnamurthy, M., Thangaramya, K., & Kannan, A. Elliptic curve encryption-based energy-efficient secured ACO routing protocol for wireless sensor networks. *J. Supercomput.* 1–34 (2024).
- Shruti, S., Rani, S., Sah, D. K. & Gianini, G. Attribute-based encryption schemes for next generation wireless IoT networks: A comprehensive survey. *Sensors* **23**(13), 5921 (2023).
- Dinesh, K. & Santhosh Kumar, S. V. N. Energy-efficient trust-aware secured neuro-fuzzy clustering with sparrow search optimization in wireless sensor network. *Int. J. Inf. Secur.* **23**(1), 199–223 (2024).
- Diarra, S., & Islam, M. S. Energy and trust-aware routing in wireless networks for multimedia applications. *Eur. J. Appl. Sci.* **12**(3) (2024).
- Raja, M., Dhanasekaran, S. & Vasudevan, V. Attribute-based encryption for ciphertext in advanced encryption standard. *Mater. Today Proc.* **37**, 3442–3445 (2021).
- Ling, J., Chen, J., Chen, J., & Gan, W. Multiauthority attribute-based encryption with traceable and dynamic policy updating. *Secur. Commun. Netw.* **2021** (2021).
- Elumalaiwasan, P., Kulothungan, K., Sannasi, G. & Arputharaj, K. Trust based ciphertext policy attribute based encryption techniques for decentralized disruption tolerant networks. *Aust. J. Basic Appl. Sci.* **10**(2), 18–26 (2016).
- Shi, Y. et al. Implementation of an attribute-based encryption scheme based on SM9. *Appl. Sci.* **9**(15), 3074 (2019).
- Begam, B. F. & Sasikala, M. Attribute based encryption in cloud computing–A. *Int. J. Comput. Appl.* **975**, 8887.
- Chung, T., & Roedig, U. DHB-KEY: An efficient key distribution scheme for wireless sensor networks. In *2008 5th IEEE International Conference on Mobile Ad Hoc and Sensor Systems* 840–846 (IEEE, 2008).
- Kwon, H., Kim, D., Hahn, C. & Hur, J. Secure authentication using ciphertext policy attribute-based encryption in mobile multipath networks. *Multimed. Tools Appl.* **76**(19), 19507–19521 (2017).
- Meng, F., Cheng, L. & Wang, M. Ciphertext-policy attribute-based encryption with hidden sensitive policy from keyword search techniques in smart city. *EURASIP J. Wirel. Commun.* **2021**(1), 1–22 (2021).
- Sicari, S. et al. Attribute-based encryption and sticky policies for data access control in a smart home scenario: A comparison on networked smart object middleware. *Int. J. Inf. Secur.* 1–19 (2020).
- Rasori, M., Perazzo, P. & Dini, G. A lightweight and scalable attribute-based encryption system for smart cities. *Comput. Commun.* **149**, 78–89 (2020).
- Mandal, M. Privacy-preserving fully anonymous ciphertext policy attribute-based broadcast encryption with constant-size secret keys and fast decryption. *J. Inf. Secur. Appl.* **55**, 102666 (2020).
- Fang, W. et al. Trust management-based and energy efficient hierarchical routing protocol in wireless sensor networks. *Digit. Commun. Netw.* (2021).
- Khan, T. & Singh, K. TASRP: A trust aware secure routing protocol for wireless sensor networks. *Int. J. Innov. Comput. Appl.* **12**(2–3), 108–122 (2021).
- Chen, S., Li, J., Zhang, Y. & Han, J. Efficient revocable attribute-based encryption with verifiable data integrity. *IEEE Internet Things J.* **11**(6), 10441–10451 (2024).
- Li, J., Zhang, E., Han, J., Zhang, Y. & Shen, J. PH-MG-ABE: A flexible policy-hidden multigroup attribute-based encryption scheme for secure cloud storage. *IEEE Internet Things J.* **12**(2), 2146–2157 (2025).
- Chen, N., Li, J., Zhang, Y. & Guo, Y. Efficient CP-ABE scheme with shared decryption in cloud storage. *IEEE Trans. Comput.* **71**(1), 175–184 (2022).
- Zhang, R., Li, J., Yang, Lu., Han, J. & Zhang, Y. Key escrow-free attribute based encryption with user revocation. *Inf. Sci.* **600**, 59–72 (2022).
- Li, J. et al. Multiauthority attribute-based encryption for assuring data deletion. *IEEE Syst. J.* **17**(2), 2029–2038 (2023).
- Li, J., Yao, W., Zhang, Y., Qian, H. & Han, J. Flexible and fine-grained attribute-based data storage in cloud computing. *IEEE Trans. Serv. Comput.* **10**(5), 785–796 (2017).

36. Bethencourt, J., Sahai, A., & Waters, B. Ciphertext-policy attribute-based encryption. In *2007 IEEE symposium on security and privacy (SP'07)* 321–334 (IEEE, 2007).
37. Nancy, P. et al. Intrusion detection using dynamic feature selection and fuzzy temporal decision tree classification for wireless sensor networks. *IET Commun.* **14**(5), 888–895. <https://doi.org/10.1049/iet-com.2019.0172> (2020).
38. Thangaramya, K. et al. Intelligent fuzzy rule-based approach with outlier detection for secured routing in WSN. *Soft Comput.* **24**(21), 16483–16497. <https://doi.org/10.1007/s00500-020-04955-z> (2020).
39. Selvi, M., Velvizhy, P., Ganapathy, S., Nehemiah, H. K. & Kannan, A. A rule based delay constrained energy efficient routing technique for wireless sensor networks. *Cluster Comput.* **22**(s5), 10839–10848. <https://doi.org/10.1007/s10586-017-1191-y> (2019).
40. Thangaramya, K. et al. Energy aware cluster and neuro-fuzzy based routing algorithm for wireless sensor networks in IoT. *Comput. Netw.* **151**, 211–223. <https://doi.org/10.1016/j.comnet.2019.01.024> (2019).
41. Rajeswari, A. R., Ganapathy, S., Kulothungan, K., & Kannan, A. An efficient trust-based secure energy-aware clustering to mitigate trust distortion attack in mobile ad-hoc network. *Concurr. Comput. Pract. Exp.* e6223 (2021).
42. Selvi, M. et al. An energy efficient clustered gravitational and fuzzy based routing algorithm in WSNs. *Wirel. Pers. Commun.* **116**(1), 61–90 (2021).
43. Han, G., Jiang, J., Shu, L., Niu, J. & Chao, H. C. Management and applications of trust in wireless sensor networks: A survey. *J. Comput. Syst. Sci.* **80**(3), 602–617. <https://doi.org/10.1016/j.jcss.2013.06.014> (2014).
44. Ren, Y., Zeng, Z., Wang, T., Zhang, S. & Zhi, G. A trust-based minimum cost and quality aware data collection scheme in P2P network. *Peer-to-Peer Netw. Appl.* **13**(6), 2300–2323. <https://doi.org/10.1007/s12083-020-00898-2> (2020).
45. Thippeswamy, B. M. et al. STEAR: Secure trust-aware energy-efficient adaptive routing in wireless sensor networks. *J. Adv. Comput. Netw.* **3**(2), 146–149. <https://doi.org/10.7763/jacn.2015.v3.157> (2015).
46. Hamdane, B., Boussada, R., Elhdhili, M. E. & El Fatmi, S. G. Hierarchical identity based cryptography for security and trust in named data networking. In *Proceedings of 2017 IEEE 26th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE 2017)* 226–231 (2017). <https://doi.org/10.1109/WETICE.2017.33>.
47. Selvi, M. et al. An energy aware trust based secure routing algorithm for effective communication in wireless sensor networks. *Wirel. Pers. Commun.* **105**(4), 1475–1490. <https://doi.org/10.1007/s11277-019-06155-x> (2019).
48. Ahmed, A., Abu Bakar, K., Channa, M. I., Haseeb, K. & Khan, A. W. A trust aware routing protocol for energy constrained wireless sensor network. *Telecommun. Syst.* **61**(1), 123–140. <https://doi.org/10.1007/s11235-015-0068-8> (2016).
49. Kalidoss, T., Rajasekaran, L., Kanagasaki, K., Sannasi, G. & Kannan, A. QoS aware trust based routing algorithm for wireless. *Wirel. Pers. Commun.* **110**(4), 1637–1658. <https://doi.org/10.1007/s11277-019-06788-y> (2020).

Author contributions

M. Selvi—Implementation Santhosh Kumar SVN-Algorithm design Thangaramya K-Paper drafting, Abdul Gafar H-Conceptualization.

Funding

Open access funding provided by Vellore Institute of Technology.

Declarations

Competing interests

The authors declare no competing interests.

Ethics approval

Authors provide the ethical approval for the given manuscript.

Consent to publish

All the authors gave permission for consent to publish.

Additional information

Correspondence and requests for materials should be addressed to M.S.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Open Access This article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

© The Author(s) 2025