frontiers | Frontiers in Medicine

ORIGINAL RESEARCH
published: 21 July 2022
doi: 10.3389/fmed.2022.829055

SecAODV: A Secure Healthcare Routing Scheme Based on Hybrid Cryptography in Wireless Body Sensor Networks

Heon Jeong[1], Sang-Woong Lee[2], Mazhar Hussain Malik[3], Efat Yousefpoor[4], Mohammad Sadegh Yousefpoor[4], Omed Hassan Ahmed[5], Mehdi Hosseinzadeh[2] and Amir Mosavi[6,7,8]**

[1] Department of Fire Service Administration, Chodang University, Muan-gun, South Korea, [2] Pattern Recognition and Machine Learning Lab, Gachon University, Seongnam, South Korea, [3] HoD Computing and IT (CIT) Global College of Engineering and Technology, Muscat, Oman, [4] Department of Computer Engineering, Dezful Branch, Islamic Azad University, Dezful, Iran, [5] Department of Information Technology, University of Human Development, Sulaymaniyah, Iraq, [6] Faculty of Civil Engineering, Technische Universität Dresden, Dresden, Germany, [7] John von Neumann Faculty of Informatics, Óbuda University, Budapest, Hungary, [8] Institute of Information Engineering, Automation and Mathematics, Slovak University of Technology in Bratislava, Bratislava, Slovakia

OPEN ACCESS

Edited by:
Brahmjit Singh, National Institute of Technology, Kurukshetra, India

Reviewed by:
Sharad Sharma, Maharishi Markandeshwar University, Mullana, India
Savita Gandhi, Gujarat University, India

***Correspondence:**
Mehdi Hosseinzadeh
mehdi@gachon.ac.kr
Amir Mosavi
amir.mosavi@mailbox.tu-dresden.de

Specialty section:
This article was submitted to Family Medicine and Primary Care, a section of the journal Frontiers in Medicine

Received: *04 December 2021*
Accepted: *08 April 2022*
Published: *21 July 2022*

Citation:
Jeong H, Lee S-W, Hussain Malik M, Yousefpoor E, Yousefpoor MS, Ahmed OH, Hosseinzadeh M and Mosavi A (2022) SecAODV: A Secure Healthcare Routing Scheme Based on Hybrid Cryptography in Wireless Body Sensor Networks. Front. Med. 9:829055. doi: 10.3389/fmed.2022.829055

In recent decades, the use of sensors has dramatically grown to monitor human body activities and maintain the health status. In this application, routing and secure data transmission are very important to prevent the unauthorized access by attackers to health data. In this article, we propose a secure routing scheme called SecAODV for heterogeneous wireless body sensor networks. SecAODV has three phases: bootstrapping, routing between cluster head nodes, and communication security. In the bootstrapping phase, the base station loads system parameters and encryption functions in the memory of sensor nodes. In the routing phase, each cluster head node calculates its degree based on several parameters, including, distance, residual energy, link quality, and the number of hops, to decide for rebroadcasting the route request (RREQ) message. In the communication security phase, a symmetric cryptography method is used to protect intra-cluster communications. Also, an asymmetric cryptography method is used to secure communication links between cluster head nodes. The proposed secure routing scheme is simulated in the network simulator version 2 (NS2) simulator. The simulation results are compared with the secure multi tier energy-efficient routing scheme (SMEER) and the centralized low-energy adaptive clustering hierarchy (LEACH-C). The results show that SecAODV improves end-to-end delay, throughput, energy consumption, packet delivery rate (PDR), and packet loss rate (PLR).

Keywords: wireless body sensor networks (WBSNs), Internet of things (IoT), secure routing, security, healthcare

1. INTRODUCTION

Recent advances in creating low-consumption electrical circuits for wireless communication allow us to produce small, low-consumption, and inexpensive equipment such as smart sensors. These intelligent sensors are devices that are installed on different objects to measure various parameters (1, 2). Sensors have different types, for example, thermal, magnetic, light, mechanical, and chemical.

They are equipped with a small battery (3, 4). Recharging this battery is very difficult because sensors are usually scattered in insecure and inaccessible environments (5, 6). Therefore, these sensors have limited energy. When a number of sensor nodes monitor the human body and control human body activities to collect health data of individuals, they create a wireless body sensor network (WBSN) (7, 8), which is shown in **Figure 1**.

Today, this advanced and efficient technology has created promising opportunities for new technologies, such as the Internet of things (IoT) (10, 11). In the IoT, each object has a digital identifier and can communicate with other objects to provide services or receive the desired services (12, 13). In IoT, smart and small objects such as bulb switches, industrial machines (14), home equipment (15), meters, vehicles (16), and human body (17) are connected to each other using the IoT platform (18, 19). In this case, they present different services such as remote monitoring of the human body physiological data, monitoring physicians and patients in hospitals, medication management in hospitals, monitoring environmental conditions, monitoring irrigation, intelligent agriculture, smart homes, and controlling road traffic (20, 21). Healthcare Internet of Things (HIoT) is a new network, which combines IoT and WBSNs. HIoT monitors patients or the elderly in the family using sensor nodes to measure parameters such as blood sugar, heart rate, blood pressure, temperature, etc. To care and control respiratory patients, such as patients with COVID-19, sensor nodes can measure their vital signs and various parameters (22, 23). As a result, physicians and nurses can be aware of the patient's health status through processing this data. Also, crowded environments (such as streets, shopping malls, and so on) can be monitored by sensor nodes in terms of light, air pressure, magnetic field, sound, and vibration to assess their health. **Figure 2** shows various HIoT applications.

In WBSNs, the routing process is very challenging because these networks have specific characteristics, such as resource constraints, unreliable communication, unsupervised operations, and lack of central management. In wireless sensor networks (WSNs), routing methods are categorized into five classes: data-centric routing, hierarchical routing, location-based routing, quality-of-service (QoS) aware routing, and secure routing. Moreover, communication security is known as a fundamental need in WBSNs because health data are very sensitive. If attackers change slightly the data, physicians analyze the wrong data and provide false treatment recommendations. On the other hand, patients tend to confidentially maintain their health information because if attackers achieve health data of patients, they may bring irreparable injuries to their personal and social life. A secure routing method should ensure data confidentiality, data integrity, authentication, and data availability when there are attacker nodes in the network. However, a secure routing scheme cannot guarantee all security requirements, but it must protect the network against routing attacks (25).

In this article, we propose a secure routing scheme called SecAODV for WBSNs. The purpose of this routing method is to improve energy consumption in the routing process and maintain security in communication links. In a secure routing scheme, the energy problem is very important because it affects directly the network lifetime. Therefore, when designing a secure

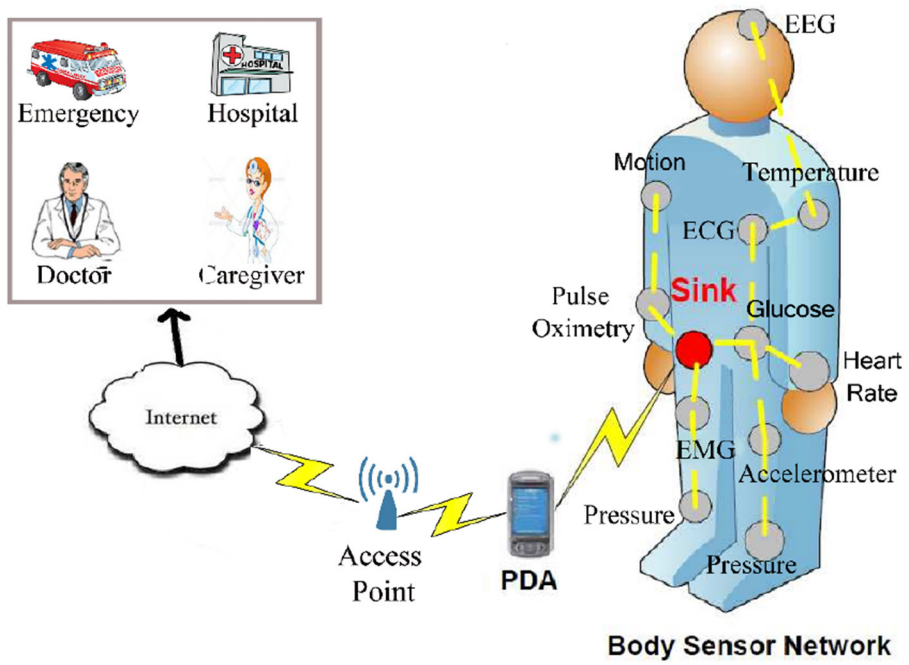

FIGURE 1 | Wireless body network and its applications (9).

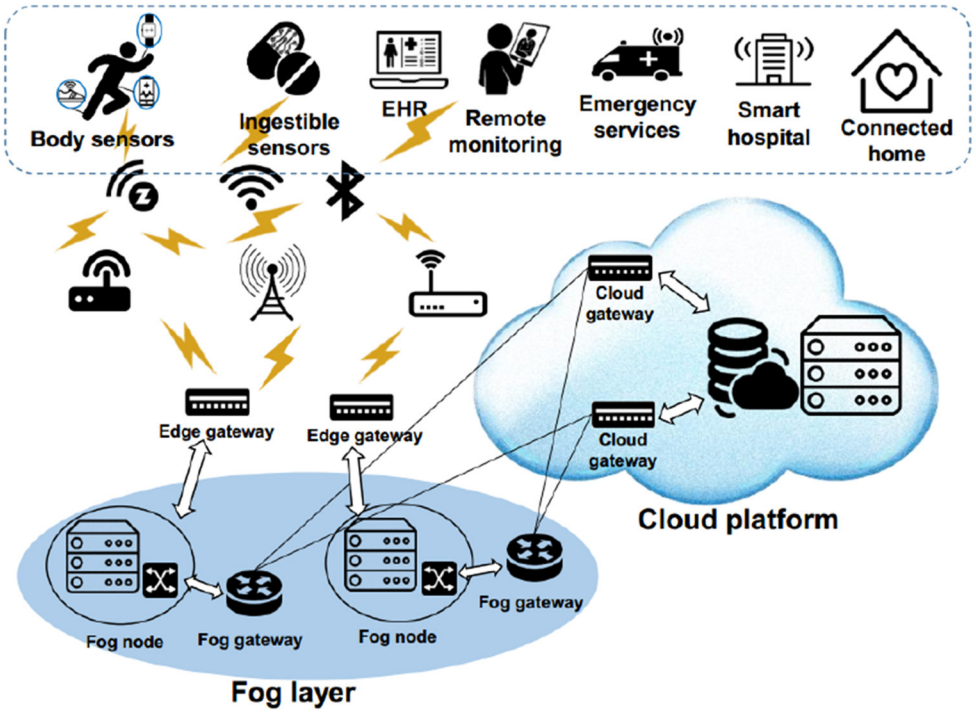

FIGURE 2 | Various HIoT applications (24).

routing method, it is necessary to reduce the energy consumption of sensor nodes. Security also has special importance in secure routing scheme in WBSNs because capturing sensor nodes by attackers affects negatively network performance. Cryptography is the most common method for maintaining data confidentiality. Symmetric key cryptography methods are desirable in terms of energy consumption, but they have a lower security level. In contrast, asymmetric key cryptography schemes guarantee better security level in the network, but they consume high energy. According to the items mentioned, SecAODV uses a hybrid key cryptography mechanism to utilize the benefits of both cryptography techniques and reduce their disadvantages. Our contributions are summarized as follows:

- We prioritize cluster head nodes (CHs) based on their degree to decide for sending the RREQ message. We calculate this degree based on the information available in the route request (RREQ) packet, including distance to the destination node, residual energy, link quality, and the number of hops. If their degree is greater than a threshold value, they rebroadcast the RREQ packet. Otherwise, the RREQ packet is deleted. This reduces communication overhead and network congestion, and balances energy consumption in the network.
- We use both key cryptography methods to secure communication links within the cluster and create a secure communication between cluster head nodes. CHs are responsible for producing the cluster key and sending it to cluster member nodes. The cluster key is a symmetric key, which is used to secure intra-cluster communications. Inter-cluster communications are also protected by asymmetric keys.
- We evaluate the performance of SecAODV and compare its results with SMEER and LEACH-C in terms of end-to-end delay, throughput, energy consumption, packet delivery rate (PDR), and packet loss rate (PLR).

In the following, the article is organized as follows: Section 2 presents the related works. In Section 3, the system model, including network model and attack model is explained. Section 4 describes the proposed secure routing scheme in detail. Section 5 analyses the security of SecAODV. Section 6 presents the simulation results of SecAODV. Finally, Section 7 concludes the article.

2. RELATED WORKS

Dhand et al. (26) presented the secure multi tier energy-efficient routing scheme (SMEER) for heterogeneous WSNs. The main goal of SMEER is to improve network security and reduce energy consumption in the network. In SMEER, sensor nodes are clustered using K-means algorithm and then the ant lion optimization algorithm (ALO) is used to select the best CH in each cluster. Clustering increases energy productivity, which boosts the network lifetime. Also, it improves the scalability of SMEER. In SMEER, an elliptic curve cryptographic (ECC) technique is used to secure data packets sent to the base station. Although, ECC increases energy consumption in the network, but it can guarantee better security. Also, the ALO algorithm

causes high computational and communication overheads in the network.

Sun et al. (27) offered the secure routing protocol based on multi-objective ant-colony-optimization (SRPMA) in WSNs. The authors modify the ant colony algorithm to become a multi-objective routing algorithm. To achieve optimal solution, SRPMA considers two optimization objectives, including trust value and remaining energy of nodes to improve network lifetime and security. To evaluate trust of nodes, SRPMA introduces a trust evaluation model based on D-S evidence theory. Although, SRPMA only focuses on two parameters, including energy and trust in the routing process and ignores other parameters such as link quality and distance between nodes. This method does not use clustering technique and is not scalable. Moreover, ACO has high communication and computational overheads, which increase energy consumption and delay in the routing process.

Yang et al. (28) suggested a secure routing scheme based on blockchain and reinforcement learning (RLBC) in WSNs. RLBC includes two main parts: routing network and blockchain network. The blockchain network is responsible for making tamper-proof and trusted routing information because it traces this information. Also, the reinforcement learning-based routing algorithm selects paths through dynamic learning of nodes. In each hop, the path information is recorded in the blockchain. Therefore, if each hop includes a routing loop, the link is invalid, or the transmission rate is low, this algorithm reduces the probability of passing through this path. As a result, RLBC can dynamically discover efficient and reliable paths. However, the reinforcement learning algorithm and the blockchain network increase computational overhead and the time complexity of RLBC. Also, it increases delay in the network. Furthermore, RLBC does not consider the energy of nodes in the routing process. RLBC has led to unbalanced energy consumption in the network. Also, RLBC ignores the clustering process in the network and is not scalable.

Shi et al. (29) proposed a secure routing scheme called IASR for WSNs. This scheme uses an improved version of the Dijkstra algorithm to secure routes despite hostile nodes in the network. IASR selects next-hop nodes based on status and trust value. The trust value defines the attack probability based on node's behavior when sending the previous packet. Status combines remaining energy and distance to the sink node. Therefore, IASR produces an optimal route with minimum cost, which is secure against hostile attacks. Moreover, IASR does not require global information when selecting a secure route. This means that IASR acts based on local information. However, IASR does not consider the clustering process in the network and is not scalable. On the other hand, in IASR, there may be paths with a high delay that is not suitable.

Mehmood et al. (30) suggested a secure and low-energy zone-based routing scheme (SeLeZoR) for WSNs. SeLeZoR divides network nodes into several zones. Then, each zone includes a number of clusters with unequal sizes. Clusters far from the base station are larger than clusters close to BS. This improves scalability, balances energy consumption, and reduces traffic in the network. Cluster member nodes are responsible for sensing the environment and sending the collected data to its CH. This process is performed with the minimum transmission power determined by the received signal strength index (RSSI). The cluster head node (CH) encrypts these data packets using a secret key and sends them to its ZH. Then, ZH sends data to the BS using a secure and efficient mechanism. SeLeZoR introduces a key management system to guarantee secure communication between the network nodes. This system generates and distributes different keys for nodes in the network. Also, this scheme efficiently utilizes the transmission channel because it applies the time division multiple access (TDMA). However, SeLeZoR uses only the symmetric key cryptography technique. Furthermore, it does not describe the key management system in detail.

Perkins et al. (31) presented the *ad hoc* on-demand distance vector (AODV) for *ad hoc* networks. In AODV, each node maintains a routing table that saves the address of the next-hop node to reach the destination. When the source node wants to send its packet to the destination node and there is no valid route, it initiates the route discovery process to find a path. To ensure that the discovered paths are free-loop, and control packets include the newest information, AODV uses a sequence number. Therefore, nodes can detect duplicated control packets caused by the flooding process. Furthermore, AODV uses a route maintenance mechanism. In AODV, when the network is large, nodes may be delayed when discovering the path. In addition, link breakage in the route discovery process leads to a lot of delay and high bandwidth consumption.

Heinzelman et al. (32) introduced an improved version of the low-energy adaptive clustering hierarchy (LEACH) called centralized LEACH (LEACH-C). It uses a centralized clustering algorithm. In LEACH-C, each node sends information about its location and energy to the base station. BS is responsible for determining appropriate clusters and balancing energy consumption in the network. In order to achieve these goals, BS calculates the average energy of nodes. If a node has less energy than the average energy, it cannot be selected as the CH node in the current iteration. BS applies the simulated annealing algorithm to select CHs. This algorithm attempts to reduce energy consumed by non-CH nodes when sending data to CH. For this purpose, it minimizes the sum of the squared distances between non-CH nodes and the nearest CH. However, WSNs are more consistent with distributed algorithms because a centralized algorithm deals with the single point of failure issue and can be subjected to various attacks.

Sathya and Umadevi (33) offered a dynamic rate aware classified key distributional secure routing (DRCKDS) for WSNs. DRCKDS categorizes data based on its sensitivity and sensor nodes based on its importance. Then, this information is used to classify and distribute secret keys. This can reduce energy consumption in the network because data with low sensitivity requires less security. Each node maintains a neighboring table that includes information about neighboring nodes such as node type, number of transfers, number of re-transfer, and its location. This information is used when discovering paths between the source node and the destination node. However, DRCKDS did not explain the routing process exactly. Finally, DRCKDS calculates the secure route measure (SRM) for each path to select

a secure route. This scale is based on the number of transfers and the number of re-transfers, which is performed by nodes in that path. However, DRCKDS does not explain how to calculate the trust value of nodes based on their behavior. Then, DRCKDS generates symmetric keys to secure the data transmission process and distributes these keys between the nodes in the path.

Mathapati et al. (34) proposed a secure routing method with multi-dimensional trust assessment for WSNs. This method presents a multi-dimensional trust assessment mechanism to evaluate the trust of nodes based on three dimensions include remaining energy, transmission pattern, and messages. Also, the authors introduce a trust recommender system to determine the compromised nodes and update the trust value. After determining the trust level of paths, a lightweight encryption system is used to provide security in the data transmission process. This reduces delay in this process. However, this method assumes that the network is not clustered and does not pay attention to scalability. In addition, this scheme does not consider parameters such as distance between the nodes, link quality, and energy in the routing process.

3. SYSTEM MODEL

In this section, we describes the assumptions related to the network model and the attack model in SecAODV.

3.1. Network Model

In SecAODV, the network model is a heterogeneous wireless body sensor network. In this method, we assume that the network is clustered by the LEACH algorithm (35). In general, the network includes a powerful, reliable, and stable base station (BS), which has sufficient energy. Furthermore, it consists of a number of cluster head nodes (CHs) with more memory capacity and processing power than other sensor nodes, and a large number of normal sensor nodes with limited energy, memory capacity, and processing power, which act as cluster member nodes (CMs). CMs sense the environment and send the collected data to its CH node. Additionally, CHs receive data from their CMs and send them to the base station. Moreover, BS is responsible for processing data and managing the network. All network nodes know the location of BS in the network. Sensor nodes in the network (CHs or CMs) are static and equipped with a global positioning system (GPS). The network model is presented in **Figure 3**.

3.2. Attack Model

An adversary node launches various attacks in the network to disrupt its performance. In this article, we focus on eavesdropping and traffic analysis attacks. Adversary node listens to all communication links and accesses the information exchanged on those links. We assume that the adversary node can capture a sensor node in the network and achieve its confidential secret keys, ID, and other critical data. Then, the attacker misuses this confidential information to capture other nodes in the network and disrupt the normal network performance. Therefore, we focus on data confidentiality in this article.

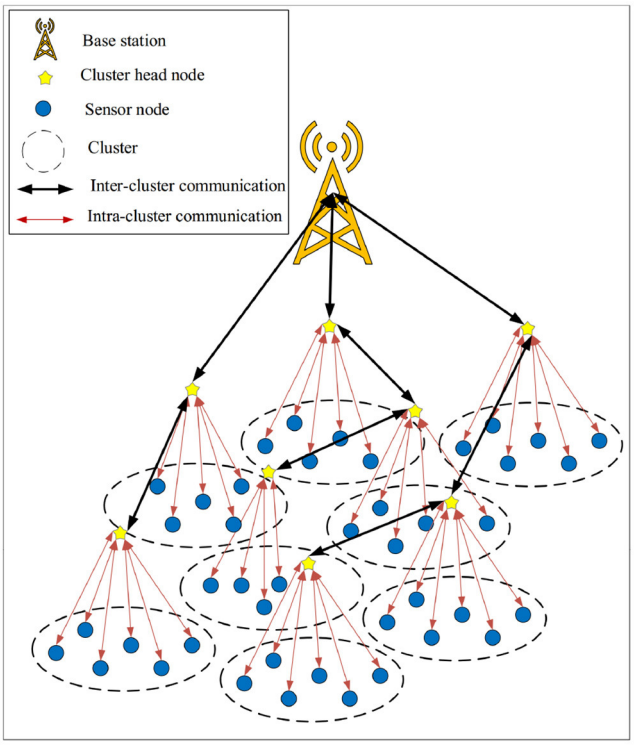

FIGURE 3 | Network model in SecAODV.

4. PROPOSED METHOD

In SecAODV, the routing process has three phases, which are described in the following:

- Bootstrapping phase
- Routing phase
- Communication security phase

4.1. Bootstrapping Phase

In this phase, BS is assigned a unique identifier (ID) and a unique key ($k_{i,BS}$) to each sensor node and loads a global key ($k_{initial}$) in the memory of nodes. $k_{initial}$ is used to protect communication between sensor nodes when bootstrapping the network. BS updates $k_{initial}$ periodically or when sensor nodes die or are compromised by attackers. Then, BS encrypts this updated key using $k_{i,BS}$ and unicasts the encrypted key only for valid nodes in the network. Moreover, BS loads some encryption parameters in the memory of CHs. Cluster head nodes use these parameters to secure communication channels in intra-cluster communication and inter-cluster communication. These parameters include:

- A key source for producing cluster key
- Public-private keys

Note that intra-cluster communication is secured by a symmetric key cryptography algorithm called the Rivest cipher 4 (RC4) and inter-cluster communication is protected using an asymmetric key cryptography algorithm called the elliptic

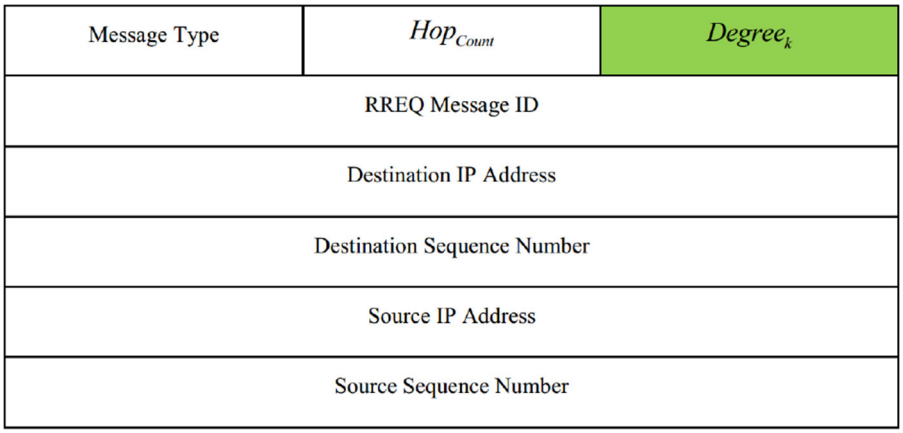

FIGURE 4 | RREQ packet template.

curve cryptographic (ECC) technique. The RC4 cipher became the most widely used stream cipher due to its speed, simplicity, and efficient implementations in both software and hardware. It is a stream cipher with a secret key whose length is 1 to 256 bytes. Also, we select ECC because this method provides better security than traditional cryptography systems at a certain key size. As a result, ECC improves system security and can increase network performance by reducing key size and energy consumption to achieve an appropriate security level.

4.2. Routing Phase

When a cluster head node (for example, CH_i) wants to send a data packet to another cluster head node ($CH_{destination}$) and there is no path to $CH_{destination}$, then CH_i begins the route discovery process. **Algorithm 1** presents the pseudocode of the routing phase in SecAODV. In the following, we describe the various steps of this algorithm in details.

In the first step (see line 1 of **Algorithm 1**), CH_i prepares a route request packet (RREQ) and adjusts its fields. Then, CH_i broadcasts this packet to its neighboring nodes. RREQ template is shown in **Figure 4**. As shown in this figure, the RREQ packet fields in SecAODV are similar to those in AODV. But there is a difference; the $Degree_k$ field, which is shown in green color. This field indicates the degree of CH node that sends the RREQ packet.

After receiving the RREQ packet, neighboring cluster head nodes (for example, CH_k) compute $Degree_k$ based on four parameters, including distance to the destination node, residual energy, link quality, and the number of hops (see line 3 of **Algorithm 1**). $Degree_k$ determines whether CH_k can replay the RREQ packet or not? CH_k can replay the RREQ packet only when it meets one of the following three modes:

- **Mode 1:** The degree of CH_k is greater than the degree of the previous-hop node ($CH_{prev-hop}$), i.e., $Degree_k \geq Degree_{pev-hop}$. Note that $Degree_{pev-hop}$ is inserted into the RREQ packet (see lines 4–6 of **Algorithm 1**).
- **Mode 2:** The degree of CH_k is more than half degree of $CH_{prev-hop}$, i.e., $Degree_k \geq \frac{1}{2} Degree_{pev-hop}$ and none of neighboring CHs rebroadcast the RREQ packet at the time $Time_{stop}$ (see lines 7–9 of **Algorithm 1**).
- **Mode 3:** A period of time equal to $\frac{3}{2} Time_{stop}$ is finished and at this time, CH_k listens to the communication channel and understands that none of neighboring CHs rebroadcast the RREQ packet (see lines 10–12 of **Algorithm 1**).

Before rebroadcasting the RREQ packet, CH_k updates Hop_{count} field and adds one unit to it. Also, it updates the $Degree_k$ field and inserts its degree in this field. This process continues until the RREQ packet reaches the destination node.

$Degree_k$ is calculated according to four parameters:

- Distance between CH_k and $CH_{destination}$ ($d_{k,destination}$): The purpose of choosing this parameter is that if the distance between CH_k and $CH_{destination}$ is low, then CH_k has more chance to be selected as the next-hop node ($CH_{next-hop}$). In this regard, whenever CH_k receives the RREQ packet, it calculates its Euclidean distance to $CH_{destination}$ based on Equation (1):

$$d_{k,destination} = \sqrt{(x_k - x_{des})^2 + (y_k - y_{des})^2} \quad (1)$$

  Where, (x_k, y_k) and (x_{des}, y_{des}) indicate the spatial coordinates of CH_k and $CH_{destination}$, respectively.
- Remaining energy (e_k): The purpose of choosing this parameter is that if CH_k has a lot of energy, then this node has gained a higher score for participating in the route formation process and have more chance to be selected as $CH_{next-hop}$. CHs are aware of their remaining energy (e_k) at any moment.
- Link quality ($q_{k,prev-hop}$): The purpose of this parameter is to create high-quality routes. Therefore, if the quality of the link between CH_k and $CH_{prev-hop}$ is high, then this node gains more score to be selected as $CH_{next-hop}$. The link quality is determined based on the received signal strength indication (RSSI) (36). Note that RSSI is a register installed on radio transmitters/receivers. RSSI calculates the signal strength when receiving the RREQ packet (37). Researchers show that

more RSSI improves PDR. Furthermore, RSSI is stable at the short period of time (about 2 s) and its standard deviation is less than 1dBm (38). For this reason, this indicator can be used to estimate link quality. When receiving the RREQ packet, CH_k estimates the quality of the link between itself and $CH_{prev-hop}$.

- Number of hops (Hop_{Count}): This parameter indicates the number of hops from the source node to the current CH node. Note that in the route formation process, routes with lower hops are better. This parameter is inserted in the RREQ packet and is added one unit in each hop.

Finally, $Degree_k$ is calculated according to Equation (2):

$$Degree_k = \left(\frac{q_{k,prev-hop} - q_{\min}}{q_{\max} - q_{\min}}\right) + \left(\frac{e_k - e_{\min}}{e_{\max} - e_{\min}}\right) + \left(1 - \frac{Hop_{Count}}{N-1}\right) + \left(1 - \frac{d_{k,destination}}{d_{\max}}\right) \quad (2)$$

Where, $q_{k,prev-hop}$ is the quality of the link between CH_k and $CH_{prev-hop}$. According to (36), when RSSI has more value, it increases PDR, which indicates a better link quality. If $q_{\max} = RSSI = 87\,dBm$, then $PDR = 99\%$. Also, when $q_{\min} = RSSI = 0\,dBm$, then $PDR = 0$. Furthermore, e_k represents the residual energy of CH_k, $e_{\max}$ indicates the initial energy of CH nodes and $e_{\min} = 0.1\,e_{\max}$. Hop_{Count} is the number of hops from the source node to CH_k. N indicates the number of sensor nodes in the network, $d_{k,destination}$ is the Euclidean distance between CH_k and $CH_{destination}$. $d_{\max}$ is determined based on the network size. Suppose that the network size is equal to $n \times m$, then $d_{\max} = \sqrt{n^2 + m^2}$.

After the RREQ packet reaches $CH_{destination}$, this node prepares a route reply packet (RREP) and sends back it to CH_{source} according to the determined path (see line 14 of **Algorithm 1**). After receiving the RREP packet, the source node inserts information about this path in its routing table. CH_{source} uses the route to send its data to $CH_{destination}$. Note that SecAODV uses a route maintenance process similar to AODV. The purpose of the route maintenance process is that a node ensures that the paths in its routing table are valid and when a route failure occurs, the node updates this failed path.

Algorithm 1: Route discovery process.

Input: N_{CH}: Number of CHs in the network.
CH_k: Cluster head nodes ($k = 1, \ldots, N_{CH}$).
Output: $Route_i$ between CH_{source} and $CH_{destination}$
Begin
1: **CH$_{source}$:** Broadcast *RREQ message* for neighboring CHs (CH_k);
2: **while** $ID_{CH_k} \neq ID_{CH_{destination}}$ **do**
3: **CH$_k$:** Calculate $Degree_k$ based on Equation (2);
4: **if** $Degree_k \geq Degree_{prev-hop}$ **then**
5: **CH$_k$:** Broadcast *RREQ message* for neighboring CHs;
6: **end if**
7: **if** $Degree_k \geq \frac{1}{2} Degree_{prev-hop}$ **and** Any CH doesn't broadcast *RREQ message* at $Time_{stop}$ **then**
8: **CH$_k$:** Broadcast *RREQ message* for neighboring CHs;
9: **end if**
10: **if** Neighboring CHs don't broadcast *RREQ message* at $\frac{3}{2} Time_{stop}$ **then**
11: **CH$_k$:** Broadcast *RREQ message* for neighboring CHs;
12: **end if**
13: **end while**
14: **CH$_k$:** Send back *RREP message* to CH_{source};
End

4.3. Communication Security Phase

In this phase, we describe how to secure communication links within the cluster and how to protect communication links between CH nodes. As mentioned in Section 4.1, we have used the RC4 cipher as a symmetric key cryptography method due to its speed, simplicity, and efficient implementations in both software and hardware.

4.3.1. Secure Intra-Cluster Communication

To provide security in communication links between cluster member nodes, we use a symmetric key cryptography method. **Algorithm 2** presents the pseudocode of the secure intra-cluster communication process. In the following, we describe the steps of this algorithm.

The CH node (for example, CH_i) is responsible for generating the cluster key and sending it to the cluster member nodes (for example, CM_j). After creating clusters and determining their members, CH_i randomly selects a key from its key source, which is loaded in the memory of CHs before distributing nodes in the network (see line 1 of **Algorithm 2**).

Then, CH_i encrypts this cluster key ($k_{cluster}$) using $k_{initial}$ and broadcasts the encrypted key to CM_j (see lines 2-3 of **Algorithm 2**). This process is expressed in Equation (3).

$$CH_i \rightarrow *: Encrypt_{k_{initial}}\left(k_{cluster}, ID_{CH_i}\right) \quad (3)$$

When CM_j receives this message, it decodes this message using $k_{initial}$, confirms the ID of CH_i and extracts $k_{cluster}$ (see line 4 of **Algorithm 2**). This process is performed according to Equation (4).

$$CM: Decrypt_{k_{initial}}\left(k_{cluster}, ID_{CH_i}\right) \quad (4)$$

Therefore, CM_j encrypts its messages ($Data_{CM_j}$) using $k_{cluster}$ and sends the encrypted message to CH_i (see lines 5-7 of **Algorithm 2**). The message encryption process is presented in Equation (5):

$$CM_j \rightarrow CH_i: Encrypt_{k_{cluster}}\left(Data_{CM_j}, ID_{CM_j}\right) \quad (5)$$

When CH_i receives the encrypted message from CM_j, it performs the decryption process, confirms the ID of CM_j and extracts $Data_{CM_j}$ from the data packet (see line 8 of **Algorithm 2**). This process is shown in Equation (6):

$$CH_i: Decrypt_{k_{cluster}}\left(Data_{CM_j}, ID_{CM_j}\right) \quad (6)$$

This process is shown in **Figure 5**.

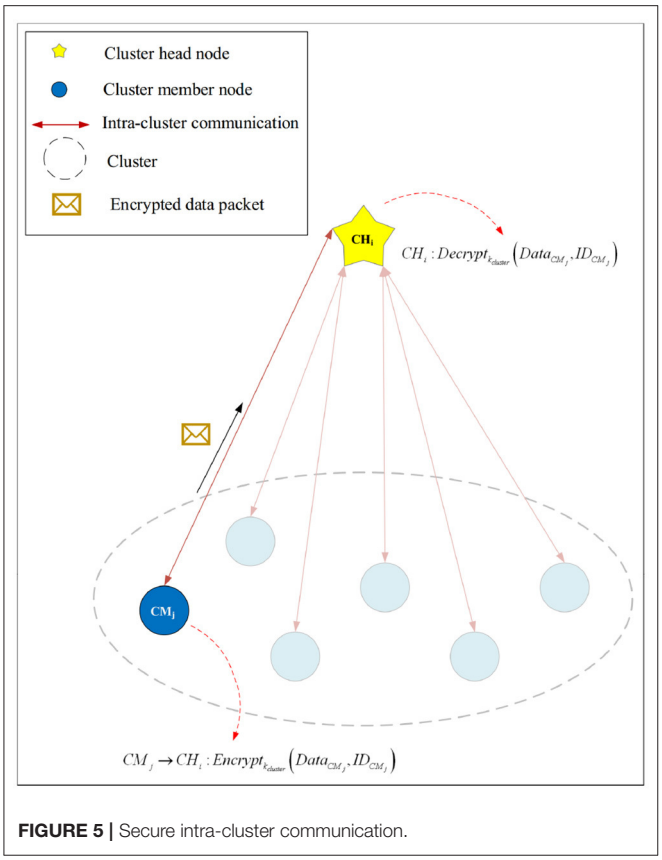

FIGURE 5 | Secure intra-cluster communication.

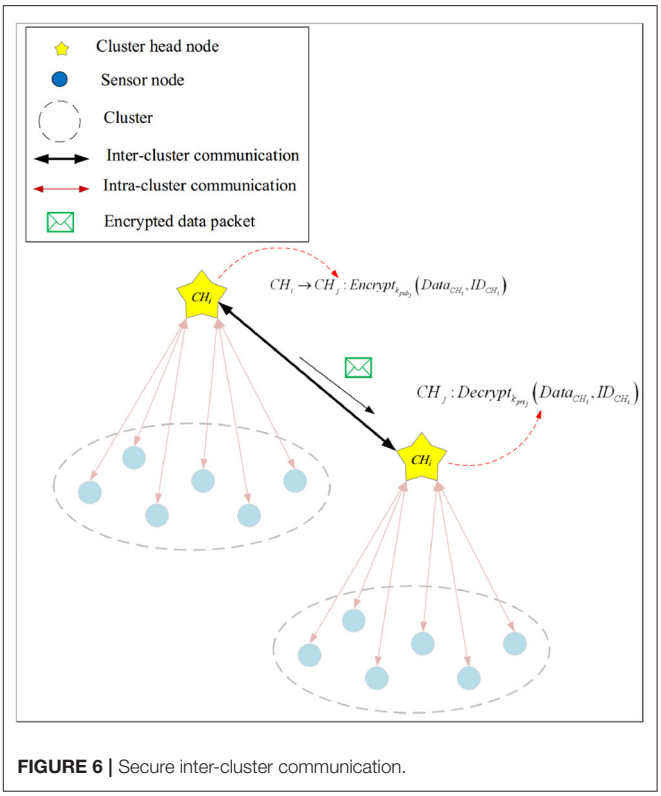

FIGURE 6 | Secure inter-cluster communication.

Algorithm 2: Secure intra-cluster communications.

Input: N_{CM}: Number of CMs in the cluster i.
CH_i: Cluster head node corresponding to the cluster i.
CM_j: CM nodes in the cluster i so that $(j = 1, \ldots, N_{CM})$.
Output: $k_{cluster}$: Cluster key
Begin
1: **CH$_i$:** Generate $k_{cluster}$;
2: **CH$_i$:** Encrypt $k_{cluster}$ using $k_{initial}$;
3: **CH$_i$:** Broadcast the encrypted $k_{cluster}$ for all CMs;
4: **CM$_j$:** Decrypt the message and extract $k_{cluster}$;
5: **if** CM_j wants to securely sent its data to CH_i **then**
6: **CM$_j$:** Encrypt its data packet ($Data_{CM_j}$) using $k_{cluster}$;
7: **CM$_j$:** Send the encrypted data packet to CH_i;
8: **CH$_i$:** Decrypt the packet using $k_{cluster}$ and extract $Data_{CM_j}$;
9: **end if**
End

4.3.2. Secure Inter-cluster Communication

CHs use an asymmetric key cryptography method called ECC to secure their communications. As stated in the bootstrapping phase, the base station produces the public-private keys ($k_{pub} - k_{pri}$) and loads them in memory of CHs before launching the network. CHs use this key to encrypt their messages. **Algorithm 3** presents the pseudocode of the secure inter-cluster communication process. In the following, we describe the steps of this algorithm.

After launching the network, each CH node shares its public key with its neighboring CHs and maintains its private key (see line 1 of **Algorithm 3**).

When CH_i wants to securely send $Data_{CH_i}$ to CH_i, it encodes this message using the public key of CH_i (k_{pub_j}) (see lines 2–4 of **Algorithm 3**). This process is presented in Equation (7):

$$CH_i \rightarrow CH_j : Encrypt_{k_{pub_j}}\left(Data_{CH_i}, ID_{CH_i}\right) \tag{7}$$

When CH_j receives this encrypted message from CH_i, it decrypts this message using its private key (k_{pri_j}) and extracts its information (see line 5 of **Algorithm 3**). This process is expressed in Equation (8).

$$CH_j : Decrypt_{k_{pri_j}}\left(Data_{CH_i}, ID_{CH_i}\right) \tag{8}$$

Also, **Figure 6** displays this process.

5. SECURITY ANALYSIS

In this section, we discuss the security of SecAODV briefly. Note that SecAODV uses a symmetric encryption technique to create a secure connection between cluster member nodes in a cluster. Also, CHs use the ECC encryption technique to protect their communications. Data confidentiality ensures that attackers cannot access sensitive information. SecAODV guarantees data confidentiality because data is encrypted in the data transmission process in a cluster. Therefore, an attacker cannot access the

Algorithm 3: Secure inter-cluster communications.

Input: CH_i: Cluster head node corresponding to the cluster i.
CH_j: Cluster head node corresponding to the cluster i.
Output: Creating a secure inter cluster communication between CH_i and CH_j.
Begin
1: **CH_i:** Broadcast its public key (k_{pub_i}) for all CHs;
2: **if** CH_i wants to securely send its data to CH_j **then**
3: **CH_i:** Encrypt $Data_{CH_i}$ using k_{pub_j};
4: **CH_i:** Send the encrypted data packet to CH_j;
5: **CH_j:** Decrypt the message using k_{pri_j} and extract $Data_{CH_i}$;
6: **end if**
End

content of the encrypted data without knowing the cluster key. Attackers do not have access to this key because CHs produce this key and securely send the cluster key to CMs. The cluster key distribution is secured using $k_{initial}$. On the other hand, attacker cannot decrypt data exchanged between CHs because they do not know the private key of CHs. Obtaining all private keys is not simple because each CH is aware of its private key and does not know the private key of other CHs. These keys are only available to the BS. Therefore, an attacker must compromise all CH nodes in the network to access their data and this is impossible. Therefore, our proposed method guarantees data confidentiality. This proves that SecAODV has a successful performance against attacks, such as eavesdropping and analytic analysis, because according to the mentioned items, if a hostile node listens to communication channels between two nodes, it cannot access information exchanged in the network. On the other hand, the proposed method has a successful performance against the capture node attack because SecAODV is a clustering-based routing method. Therefore, if an attacker compromises a cluster member node, this attack affect locally inside the cluster, and other communications are secure in the whole network. In addition, if the attacker captures a CH node, it achieves only its information and cannot disrupt secure communications between other CHs.

6. SIMULATION OF THE PROPOSED METHOD

In this section, we evaluate the performance of SecAODV. First, the proposed routing scheme is simulated using the NS-Allinone-2.35 simulator. Then, the simulation results are compared with two routing methods, including SMEER (26) and LEACH-C (32). In the simulation process, we assume that there are 100 sensor nodes, which are randomly scattered in the network with a size of $2,500 \times 50\ m^2$. These nodes do not move. The BS is located at the network center. The packet size is 1024 bits. The initial energy of normal sensor nodes and CH nodes are considered 0.5 and 1 J, respectively. Furthermore, we consider the simulation time equal to 30 s. Other simulation parameters are summarized in **Table 1**. In the simulation process, we compare our scheme with SMEER and LEACH-C in terms of end-to-end delay, throughput, energy consumption, packet delivery rate (PDR), and packet loss rate (PLR).

TABLE 1 | Simulation parameters.

Parameter	Value
Simulator	NS-2.35
Network size	$50 \times 2,500\ m^2$
Location of BS	Network center
Total number of sensor nodes	100
Initial energy of CHs	1 J
Initial energy of sensor nodes	0.5 J
Antenna	Omni-Antenna
Packet size	1024 bit
Mac protocol	IEEE 802.11
Simulation time	30 s
Black hole nodes	5

6.1. End-To-End Delay

This parameter is defined as the sum of the time required to deliver the data packet to the recipient node. This parameter is obtained using Equation (9).

$$End - to - end\ delay = \frac{Sum\ of\ time\ taken\ to\ deliver\ packet\ in\ receiver}{Noumber\ of\ packet\ received\ by\ receiver} \quad (9)$$

Figure 7 compares end-to-end delay in different routing methods. As shown in this figure, SecAODV has the lowest delay in comparison with other routing methods. On average, our scheme decreases delay by 10.07 and 21.04% compared to SMEER and LEACH-C, respectively. As a result, SecAODV performs the data transmission process more quickly. This issue has several reasons: (1) SMEER uses only asymmetric encryption method to secure the data transfer process. This increases delay in this process. While SecAODV uses a hybrid cryptography scheme. In our proposed method, the symmetric key cryptography is used to build secure communication between cluster member nodes. So that CMs encrypt their data using the cluster key and send it to its CH. Also, the secure connection between CHs is guaranteed using an asymmetric key cryptography technique. (2) SMEER uses the ALO algorithm in the clustering process. This increases highly computational overhead and needs high iterations to find optimal response. These items increase delay and weaken the network performance. Additionally, LEACH-C uses the simulated annealing algorithm in the clustering process. It increases computational overhead and delay. In contrast, SecAODV utilizes the LEACH algorithm for clustering. It is faster than the other two methods. (3) SecAODV considers link quality and energy of the nodes. Therefore, it can create more stable routes than SMEER and LEACH-C. This reduces route failure. As a result, our scheme lowers delay in the routing process.

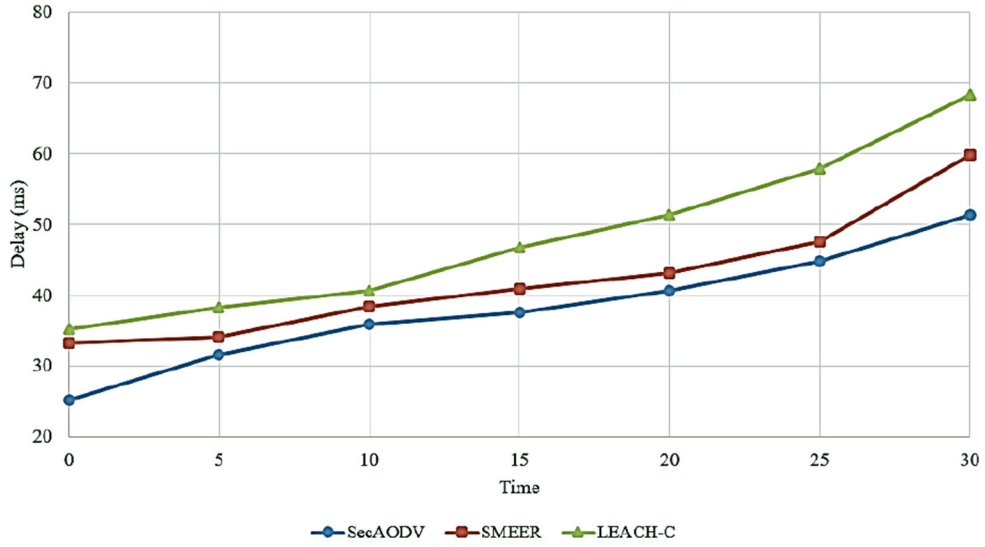

FIGURE 7 | Comparison of different method in terms of delay.

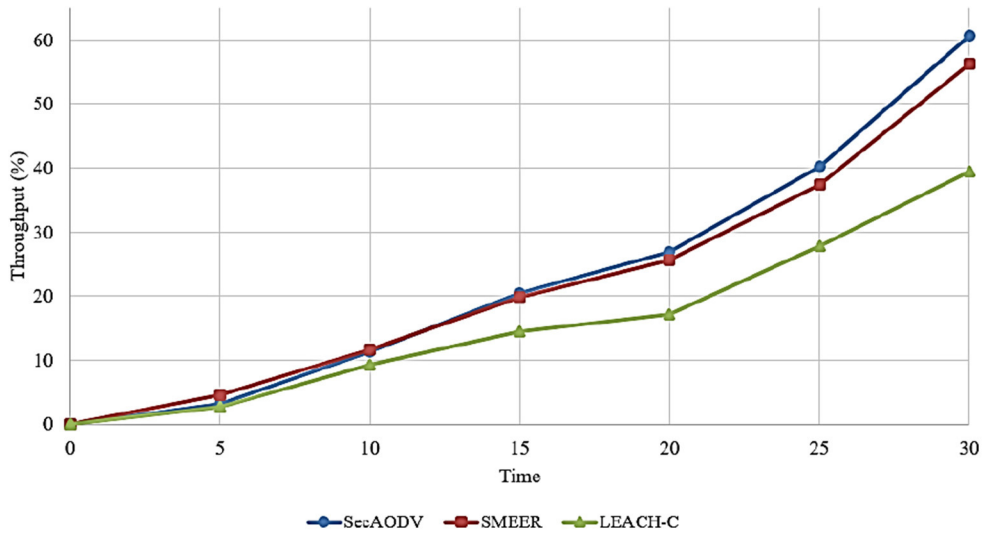

FIGURE 8 | Comparison of different methods in terms of throughput.

6.2. Throughput

This parameter is defined as the ratio of data packets received at the receiver node to delay required for transferring these packet. This parameter is calculated based on Equation (10):

$$Throughput = \frac{Number\ of\ packets\ received}{Delay} \tag{10}$$

Figure 8 compares different routing methods in terms of throughput. As shown in this figure, SecAODV has the best throughput compared to other routing methods because it improves throughput by 4.83 and 46.85% compared to SMEER and LEACH-C, respectively. This is because SecAODV has less delay than other routing methods in the data transmission process. We presented its reasons in Section 6.1. Secondly, in the routing process, SecAODV attempts to find high-energy nodes for creating paths. Furthermore, it creates high-quality routes with fewer hops. As a result, SecAODV facilitates the data transfer process and improves throughput.

6.3. Energy Consumption

This parameter is expressed as the sum of the required energy for receiving a packet and the required energy for sending the packet in the data transfer process. **Figure 9** compares different routing

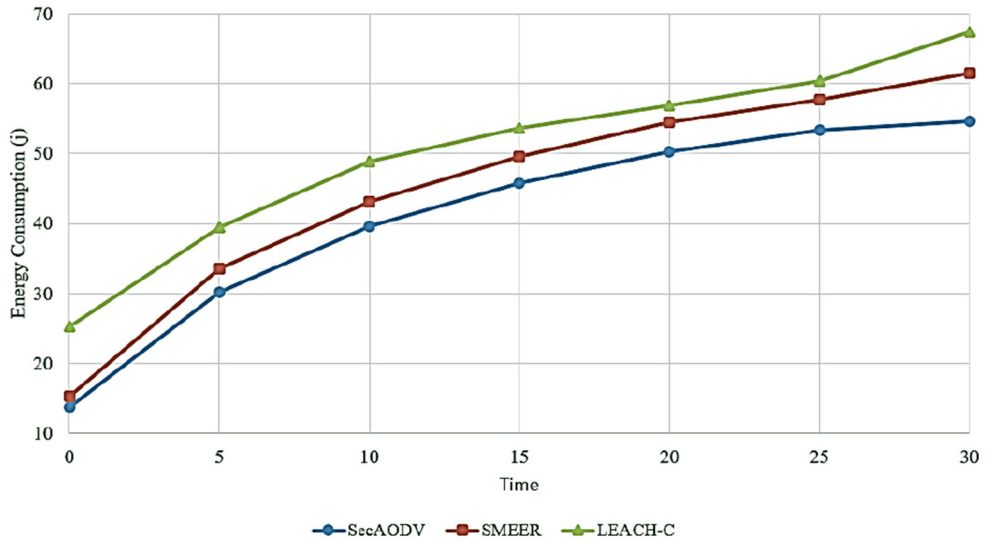

FIGURE 9 | Comparison of different methods in terms of energy consumption.

methods in terms of energy consumption. As shown in this figure, SecAODV has the lowest energy consumption compared to other methods because it has reduced energy consumption by 8.82 and 18.31% compared to SMEER and LEACH-C, respectively. This has several reasons: firstly, in LEACH-C, CHs communicate with the BS in a single-hop manner. This increases energy consumption dramatically. On the other hand, SMEER performs the routing process in a multi-hop manner. This improves energy consumption. However, SMEER considers two parameters, including distance and the angle between nodes when selecting the next-hop node. Choosing more appropriate parameters can improve the performance of this routing method. In SecAODV, CHs communicate with the BS in a multi-hop manner. Also, it considers various parameters, including energy, distance, link quality, and the number of hops, when selecting the next-hop node. As a result, it creates more stable paths and reduces the packet loss rate. This improves energy consumption in the data transmission process.

6.4. Packet Loss Rate

This parameter is defined as the percentage of data packets that are not reached at the destination. This parameter is obtained according to Equation (11).

$$PLR = \frac{\sum_{i=1}^{n} P_l}{\sum_{i=1}^{n} P_s} \times 100 \tag{11}$$

Where, P_l is packets that are not reached at the destination and P_s is packets sent by the source node.

Figure 10 compares different routing methods in terms of PLR. As shown in this figure, SecAODV has the lowest PLR compared to others because it has reduced PLR by 31.43 and 55.14% compared to SMEER and LEACH-C, respectively. LEACH-C has the worst PLR because CHs has high communication overhead and consume a lot of energy. They must receive data from its CM nodes and send directly the data to the BS. This can increase the packet loss rate. On the other hand, SMEER considers only two parameters, including distance and angle between neighbor nodes in the route discovery process. While, considering energy and link quality is very important. Therefore, SMEER may create unstable routes. This can increase PLR. In SecAODV, we take into account energy and link quality in the route discovery process to create more stable paths and reduce PLR.

6.5. Packet Delivery Rate

This parameter is introduced as the ratio of the data packets received by the receiver to the total number of packets. This parameter is obtained according to Equation (12).

$$PDR = \frac{\sum_{i=1}^{n} P_r}{\sum_{i=1}^{n} P_s} \times 100 \tag{12}$$

Where, P_r is packets received by the destination node and P_s is packets sent by the source node.

Different routing methods have been compared in terms of PDR in **Figure 11**. As shown in this figure, SecAODV has the best packet delivery rate compared to other routing methods because it improves PDR by 13.83 and 32.1% compared to SMEER and LEACH-C, respectively. This shows that our proposed method facilitates the data transmission

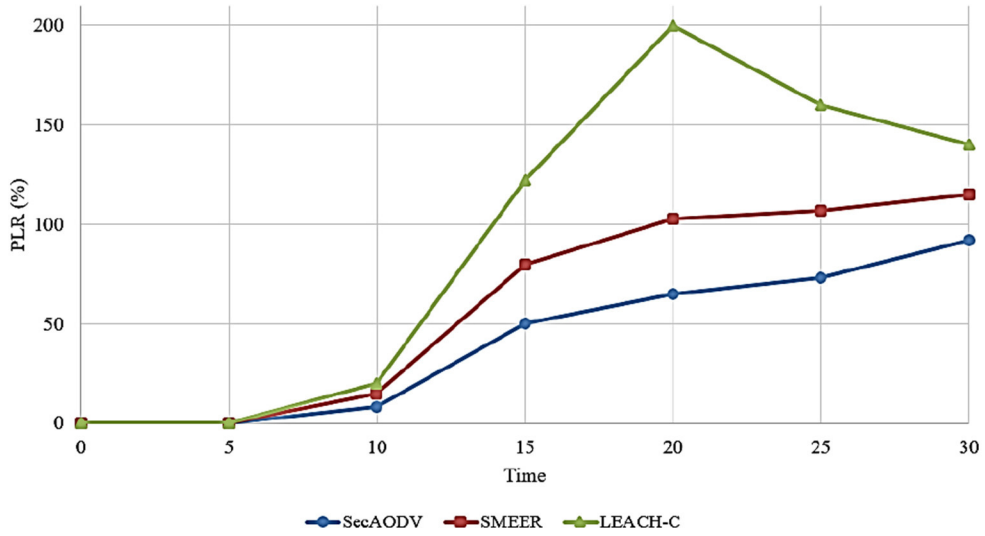

FIGURE 10 | Comparison of different methods in terms of PLR.

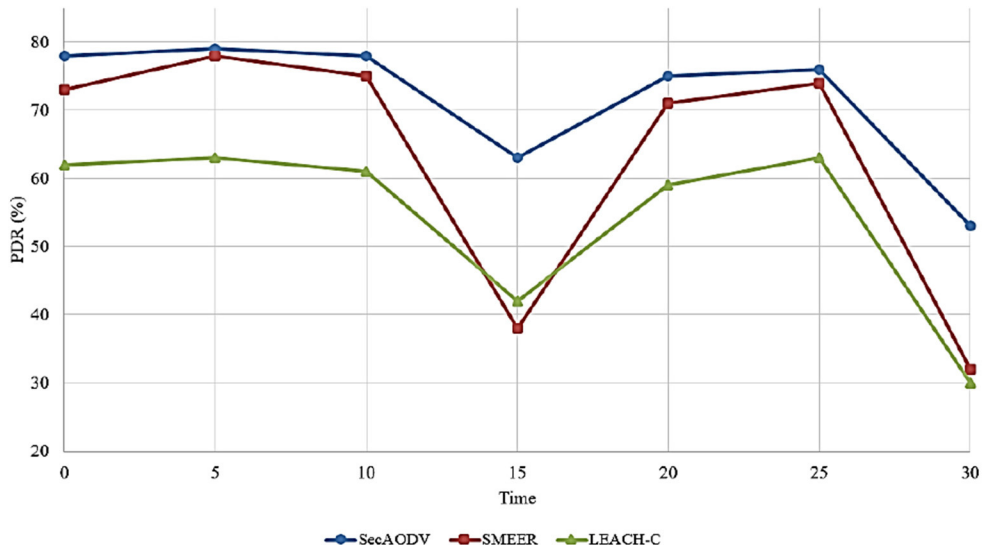

FIGURE 11 | Comparison of different methods in terms of PDR.

process and improves throughput. We stated its reasons in Section 6.4.

7. CONCLUSION

In this article, we proposed a secure routing scheme called SecAODV for heterogeneous WBSNs. The proposed method consists of three phases: bootstrapping, routing, and communication security. In the routing phase, we managed the RREQ replay process using a parameter called node degree. This helps SecAODV to form high-energy and high-quality paths with fewer hops between source and destination nodes. Furthermore, in the security phase, we introduced a hybrid cryptography scheme and described the key production and distribution processes. Then, SecAODV was simulated using the NS2 simulator. Finally, its results were compared with SMEER and LEACH-C in terms of end-to-end delay, throughput, energy consumption, packet delivery rate, and packet loss rate. The simulation results show that SecAODV outperforms SMEER and LEACH-C. Our scheme reduces energy consumption and delay

in the data transfer process. Also, it improves throughput and provides high PDR. In future research, we attempt to strengthen security in SecAODV using powerful key encryption techniques. Also, we add an authentication mechanism to SecAODV in healthcare to prevent false packet injection or control message modification by attackers in the route discovery process. In addition, secure routing methods can be designed using some artificial intelligence techniques such as artificial neural networks (ANN), machine learning (ML) techniques, and evolutionary algorithms (EA) to achieve good results.

DATA AVAILABILITY STATEMENT

The original contributions presented in the study are included in the article/supplementary material, further inquiries can be directed to the corresponding author/s.

AUTHOR CONTRIBUTIONS

All authors listed have made a substantial, direct, and intellectual contribution to the work and approved it for publication.

REFERENCES

1. Yousefpoor E, Barati H, Barati A. A hierarchical secure data aggregation method using the dragonfly algorithm in wireless sensor networks. *Peer Peer Network Appl*. (2021) 14:1917–42. doi: 10.1007/s12083-021-01116-3
2. Yousefpoor MS, Yousefpoor E, Barati H, Barati A, Movaghar, Hosseinzadeh A, et al. Secure data aggregation methods and countermeasures against various attacks in wireless sensor networks: a comprehensive review. *J Netw Comput Appl*. (2021) 2021:103118. doi: 10.1016/j.jnca.2021.103118
3. Rahmani AM, Yousefpoor E, Yousefpoor MS, Mehmood Z, Haider A, Hosseinzadeh M, et al. Machine Learning (ML) in medicine: review, applications, and challenges. *Mathematics*. (2021) 9:2970. doi: 10.3390/math9222970
4. Uchiteleva E, Hussein, Shami AR. A. Lightweight dynamic group rekeying for low-power wireless networks in IIoT. *IEEE Internet Things J*. (2020) 7:4972–86. doi: 10.1109/JIOT.2020.2974839
5. Yousefpoor S, Barati MH. DSKMS: a dynamic smart key management system based on fuzzy logic in wireless sensor networks. *Wireless Netw*. (2020) 26:2515–35. doi: 10.1007/s11276-019-01980-1
6. Rahmani AM, Ali S, Yousefpoor MS, Yousefpoor E, Naqvi RA, Siddique, et al. An area coverage scheme based on fuzzy logic and shuffled frog-leaping algorithm (SFLA) in heterogeneous wireless sensor networks. *Mathematics*. (2021) 9:2251. doi: 10.3390/math9182251
7. Awotunde JB, Jimoh RG, Abdul Raheem M, Oladipo ID, Folorunso M, Ajamu SO. IoT-based wearable body sensor network for COVID-19 pandemic. In: *Advances in Data Science and Intelligent Data Communication Technologies for COVID-19*. (2022). p. 253–75. doi: 10.1007/978-3-030-77302-1_14
8. Lin K, Li Y, Sun J, Zhou Q, Zhang D. Multi-sensor fusion for body sensor network in medical human-robot interaction scenario. *Inform Fusion*. (2020) 57:15–26. doi: 10.1016/j.inffus.2019.11.001
9. Ayatollahitafti V, Ngadi MA, Sharif JBM, Abdullahi M. An efficient next hop selection algorithm for multi-hop body area networks. *PLoS ONE*. (2016) 11:e0146464. doi: 10.1371/journal.pone.0146464
10. Yousefpoor H, Barati MS. Dynamic key management algorithms in wireless sensor networks: a survey. *Comput Commun*. (2019) 134:52–69. doi: 10.1016/j.comcom.2018.11.005
11. Chaeikar SS, Alizadeh M, Tadayon A, Jolfaei MH. An intelligent cryptographic key management model for secure communications in distributed industrial intelligent systems. *Int J Intell Syst*. (2021) 1–14. doi: 10.1002/int.22435
12. Lee SW, Ali S, Yousefpoor MS, Yousefpoor E, Lalbakhsh PM, Javaheri D, et al. An energy-aware and predictive fuzzy logic-based routing scheme in flying *ad hoc* networks (FANETs). *IEEE Access*. (2021) 9:129977–30005. doi: 10.1109/ACCESS.2021.3111444
13. Tange K, De Donno M, Fafoutis N, Dragoni X. A systematic survey of industrial Internet of Things security: requirements and fog computing opportunities. *IEEE Commun Surv Tutor*. (2020) 22:2489–520. doi: 10.1109/COMST.2020.3011208
14. Liu M, Yang K, Zhao N, Chen Y, Song F, Gong H. Intelligent signal classification in industrial distributed wireless sensor networks based industrial internet of things. *IEEE Trans Indus Inform*. (2020) 17:4946–56. doi: 10.1109/TII.2020.3016958
15. Nizetic S, Solic P, Gonzalez-de-Artaza DL, Patrono L. Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future. *J Clean Product*. (2020) 274:122877. doi: 10.1016/j.jclepro.2020.122877
16. Stoyanova M, Nikoloudakis Y, Panagiotakis S, Pallis EK, Markakis E. A survey on the internet of things (IoT) forensics: challenges, approaches, open issues. *IEEE Commun Surv Tutor*. (2020) 22:1191–221. doi: 10.1109/COMST.2019.2962586
17. Qadri YA, Nauman A, Zikria YB, Vasilakos SW, Kim AV. The future of healthcare internet of things: a survey of emerging technologies. *IEEE Commun Surv Tutor*. (2020) 22:1121–67. doi: 10.1109/COMST.2020.2973314
18. Cao B, Wang X, Zhang W, Song Z, Lv H. A many-objective optimization model of industrial internet of things based on private blockchain. *IEEE Netw*. (2020) 34:78–83. doi: 10.1109/MNET.011.1900536
19. Hui H, Zhou C, Xu F, Lin S. A novel secure data transmission scheme in industrial internet of things. *China Commun*. (2020) 17:73–88. doi: 10.23919/JCC.2020.01.006
20. Abuhasel MA, Khan KA. A secure industrial internet of things (IIoT) framework for resource management in smart manufacturing. *IEEE Access*. (2020) 8:117354–64. doi: 10.1109/ACCESS.2020.3004711
21. Qureshi KN, Rana SS, Ahmed G, Jeon A. A novel and secure attacks detection framework for smart cities industrial internet of things. *Sustain Cities Soc*. (2020) 61:102343. doi: 10.1016/j.scs.2020.102343
22. Pandey C, Sharma P, Matta S. Privacy techniques for body sensor network in healthcare internet of things (HIoT)-a critical survey. In: *5th International Conference on Computing Methodologies Communication (ICCMC)*. Erode: IEEE (2021). p. 385–9. doi: 10.1109/ICCMC51019.2021.9418484
23. Aggarwal A, Gandhi S, Chaubey N, Shah M, Sadhwani P. ODVSEC: a novel approach to secure *Ad Hoc* on-Demand Distance Vector (AODV) routing protocol from insider attacks in MANETs. *arXiv preprint arXiv:1208.1959*. (2012). doi: 10.5121/ijcnc.2012.4412
24. Dang LM, Piran M, Han D, Min H, Moon K. A survey on internet of things and cloud computing for healthcare. *Electronics*. (2019) 8:768. doi: 10.3390/electronics8070768
25. Chan L, Chavez KG, Rudolph A, Hourani H. Hierarchical routing protocols for wireless sensor network: a compressive survey. *Wireless Netw*. (2020) 26:3291–314. doi: 10.1007/s11276-020-02260-z
26. Dhand SS, Tyagi G. SMEER: secure multi-tier energy efficient routing protocol for hierarchical wireless sensor networks. *Wireless Pers Commun*. (2019) 105:17–35. doi: 10.1007/s11277-018-6101-y
27. Sun Z, Wei M, Zhang G, Qu Z. Secure routing protocol based on multi-objective ant-colony-optimization for wireless sensor networks. *Appl Soft Comput*. (2019) 77:366–75. doi: 10.1016/j.asoc.2019.01.034
28. Yang J, He S, Xu Y, Chen J, Ren L. A trusted routing scheme using blockchain and reinforcement learning for wireless sensor networks. *Sensors*. (2019) 19:970. doi: 10.3390/s19040970
29. Shi Q, Qin L, Ding Y, Xie B, Zheng L, Song J. Information-aware secure routing in wireless sensor networks. *Sensors*. (2020) 20:165. doi: 10.3390/s20010165
30. Mehmood A, Lloret S, Sendra J. A secure and low-energy zone-based wireless sensor networks routing protocol for pollution monitoring. *Wireless Commun Mobile Comput*. (2016) 16:2869–83. doi: 10.1002/wcm.2734
31. Perkins EM, Royer CE. *Ad-hoc* on-demand distance vector routing. In: *Proceedings WMCSA'99. Second IEEE Workshop on Mobile Computing*

Systems Applications. IEEE (1999). p. 90–100. doi: 10.1109/MCSA.1999.749281
32. Heinzelman WB, Chandrakasan H, Balakrishnan AP. An application-specific protocol architecture for wireless microsensor networks. *IEEE Trans Wireless Commun*. (2002) 1:660–70. doi: 10.1109/TWC.2002.804190
33. Sathya K, Umadevi SS. An optimized distributed secure routing protocol using dynamic rate aware classified key for improving network security in wireless sensor network. *J Ambient Intell Human Comput*. (2021) 12:7165–71. doi: 10.1007/s12652-020-02392-2
34. Mathapati M, Kumaran TS, Muruganandham M, Mathivanan A. Secure routing scheme with multi-dimensional trust evaluation for wireless sensor network. *J Ambient Intell Human Comput*. (2021) 12:6047–55. doi: 10.1007/s12652-020-02169-7
35. Heinzelman WR, Chandrakasan H, Balakrishnan A. Energy-efficient communication protocol for wireless microsensor networks. In: *Proceedings of the 33rd Annual Hawaii International Conference on System Sciences*. IEEE (2000). p. 10.
36. Baccour N, Koubca A, Mottola L, Zuniga MA, Youssef H, Boano M, et al. Radio link quality estimation in wireless sensor networks: a survey. *ACM Trans Sensor Netw*. New York, NY (2012) 8:1–33. doi: 10.1145/2240116.2240123
37. Lowrance AP, Lauf CJ. Link quality estimation in *ad hoc* and mesh networks: a survey and future directions. *Wireless Pers Commun*. (2017) 96:475–508. doi: 10.1007/s11277-017-4180-9
38. Vlavianos A, Law LK, Broustis I, Krishnamurthy M, Faloutsos SV. Assessing link quality in IEEE 802.11 wireless networks: which is the right metric? In: *2008 IEEE 19th International Symposium on Personal, Indoor Mobile Radio Communications*. Cannes: IEEE (2018). p. 1–6. doi: 10.1109/PIMRC.2008.4699837

Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.