Robust and Secure Routing Protocol Based on Group Key Management for Internet of Things Systems

Salwa Othmen
Computers and Information Technology Department, College of Science and Arts Turaif, Northern Border University, Saudi Arabia
salwaothmen@gmail.com (corresponding author)

Wahida Mansouri
Computers and Information Technology Department, College of Science and Arts Turaif, Northern Border University, Saudi Arabia
wahidamn@gmail.com

Somia Asklany
Computers and Information Technology Department, College of Science and Arts Turaif, Northern Border University, Saudi Arabia
somia.as@yahoo.fr

Received: 21 February 2024 | Revised: 13 March 2024 | Accepted: 18 March 2024

 DOI: https://doi.org/10.48084/etasr.7115

ABSTRACT

The Internet of Things (IoT) has significantly altered our way of life, being integrated into many application types. These applications require a certain level of security, which is always a top priority when offering various services. It is particularly difficult to protect the information produced by IoT devices from security threats and protect the exchanged data as they pass through various nodes and gateways. Group Key Management (GKM) is an essential method for controlling the deployment of keys for network access and safe data delivery in such dynamic situations. However, the huge volume of IoT devices and the growing subscriber base present a scalability difficulty that is not addressed by the current IoT authentication techniques based on GKM. Moreover, all GKM models currently in use enable the independence of participants. They only concentrate on dependent symmetrical group keys for each subgroup, which is ineffective for subscriptions with very dynamic behavior. To address these issues, this study proposes a unique Decentralized Lightweight Group Key Management (DLGKM) framework integrated with a Reliable and Secure Multicast Routing Protocol (REMI-DLGKM), which is a reliable and efficient multicast routing system for IoT networks. REMI-DLGKM is a cluster-based routing protocol that qualifies for faster multiplex message distribution within the system. According to simulation results, this protocol is more effective than cutting-edge protocols in terms of end-to-end delay, energy consumption, and packet delivery ratio. The packet delivery ratio of REMI-DLGKM was 99.21%, which is 4.395 higher than other methods, such as SRPL, QMR, and MAODV. The proposed routing protocol can reduce energy consumption in IoT devices by employing effective key management strategies.

Keywords-Internet of Things (IoT); Reliable and Secure Multicast Routing Protocol for IoT Networks (REMI-DLGKM); Decentralized Lightweight Group Key Management (DLGKM); Group Key Management (GKM)

I. INTRODUCTION

Today, when numerous programs or computers communicate, shared access to applications or files can be abused [1]. Most of these applications use secured multicasting. Group Key Management (GKM) considers authentication and privacy. Implementing cryptographic encryption and the selective exchange of keys emploued to encrypt data could limit the accessibility to communication by unauthorized individuals. A secret group key is essential for several secured group communications [2]. The confidentiality of the message is guaranteed by encryption employing a group key only known to authorized users. A variety of potential hazards related to the confidentiality and reliability of the keys deployed for encryption cannot be managed without efficient key management. Therefore, group keys must be upgraded to

provide the right to admission management on variable multicast networks where users join and leave. Otherwise, the key can be manipulated by an unauthorized user and endanger forward and backward confidentiality [3]. A single user can create and transmit a message to an entire network group implementing communication protocols, which is more effective than a comparable unicast-based solution, following a group communication concept [4]. Internet gaming and audio/video broadcasting were among the initial ways to utilize the group communications concept to their advantage. Ad hoc (primarily wireless) networks have become increasingly prevalent recently, creating a healthy environment for new group-based services. Many applications, such as data transmission, peer-to-peer communications, and data collection, in contexts that include wireless sensor networks, mobile ad hoc networks, and IoT, require a robust multicast data delivery service [5].

Ensuring secrecy and reliability for messages transmitted within a group utilizing appropriate cryptography solutions without compromising multicast transmissions is the foundation of protecting group interactions [6]. It is difficult to accomplish this goal in an effective and scalable way, as it requires a sizable and constantly shifting number of users to share cryptographic keys, even when there are unreliable membership changes brought on by users joining or leaving the system. Common cryptographic resources must be updated using a proper rekeying process after every membership change, preventing a former group member from accessing the group's present communications and a new member from accessing the group's previous messages [7]. While asymmetric encryption, such as in conventional point-to-point communications, makes it simple to maintain the reliability and legitimacy of group interactions, the simplest and most adaptable way to ensure the privacy of information within multiplex grouping is to secure the information deploying symmetric cryptography, with a secret key utilized by every group member. The group key is the typical term adopted to describe these symmetric keys [8].

According to the security strategy imposed on the group, key management is essential to establish and maintain significant connections between legitimate users [9]. It consists of techniques and actions that can deliver some provisions, including access control, member authentication and authorization, and key generation, distribution, and deployment. Key storage and key updates are crucial procedures in the key management framework [10]. A key management strategy should address the costs associated with that procedure. If there is an alteration in the registration, an effective multiplex with appropriate access handles the procedure that could be accomplished by a suitable update of the group key [11]. The affected keys can be changed through a process called rekeying. The quantity of rekeying becomes the main bottleneck as the community grows and/or the number of membership changes increases. Group rekeying has been proposed to address the issue of regular rekeying. In this method, the key server waits first for a time known as the rekeying period before processing the rekeying process [12].

The routing protocol for low-power and lossy networks (RPL) supports Point-to-Point (P2P) communications. P2M routing could be more advantageous for most real-world IoT applications, including home and security administration automation, environment monitoring, and smart energy tracking [13]. Additionally, since only one route is available in RPL connecting the source network and any other destination node, communication security and reliability represent major challenges to effective communication. REMI is a new and reliable cluster-based multicast routing technology suggested for lossy low-power networking [14]. An intercluster communications approach that rapidly distributes multicast packets in an orderly and effective manner is an essential feature of REMI [15]. The protocol aims to reduce the overhead of the number of messages transmitted between group members while maintaining a sufficient security level [16]. This protocol delivers outstanding performance assuming low eviction rates and can be used in highly complex settings involving a significant number of nodes (thousands).

The Secure Routing Protocol for Low-Power and Lossy Networks (SRPL) is intended for low-power and lossy IoT network settings [17]. Through the integration of secure data transfer techniques, this protocol puts a high priority on communication security. By following effective routing strategies that are appropriate for devices with limited resources, SRPL ensures that communication in IoT networks is safe and energy efficient. It solves the problems brought on by the special qualities of lossy and low-power networks, making it a good option for IoT applications where security and energy efficiency are important factors. Enhancing the quality of multicast communication in networks is the main goal of Quality-based Multicast Routing (QMR) [18]. This approach aims to maximize message delivery while taking into account latency, dependability, and resource usage. QMR aims to improve multicast communication performance by deploying quality-based routing decisions, making them appropriate for situations where efficient data delivery to numerous locations is crucial. The protocol's ability to adapt to shifting network circumstances and offer the best possible balance between quality indicators helps to increase communication reliability.

The proactive routing protocol Mobile Ad Hoc On-Demand Distance Vector (MAODV) was created for Mobile Adhoc Networks (MANETs) [19]. Creating routes as needed reduces the overhead involved in keeping the network architecture consistent. The dynamic character of MANETs, in which nodes can join, depart, or move around at any time, is well accommodated by MAODV. This protocol allows for the dispersed maintenance of route information, which enables prompt adaptation to dynamic network conditions. Although MAODV works well in situations with mobile devices and dynamic network topologies, its effectiveness can change with node mobility and network size.

Figure 1 shows a classification of GKM schemes. A central organization known as the Key Distribution Center (KDC) or group controller is in charge of creating and dispersing the group keys in a scheme known as centralized key management. Distributed key management systems eliminate the requirement

for a central authority by distributing key management duties among group members [20].

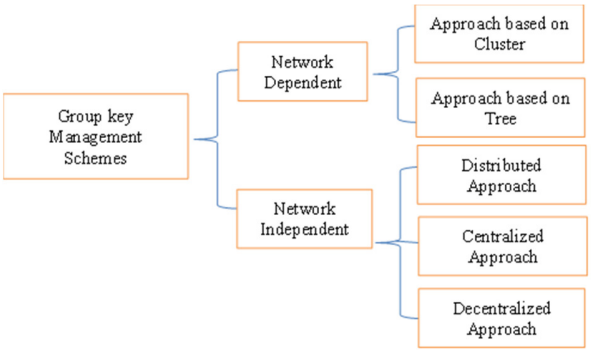

Fig. 1. Group Key Management (GKM) schemes.

The key contributions of this study are:

- Propose a robust and secure routing protocol that combines cutting-edge security features specifically designed for the special difficulties in IoT systems. The protocol should guarantee secure communication in IoT by utilizing GKM, mitigating vulnerabilities and possible threats unique to this dynamic and resource-constrained context.
- Use GKM in the proposed routing protocol. By guaranteeing that only authorized devices within a group can access and interpret the sent data, this method improves overall communication security and protects against potential security breaches and unauthorized access.
- Demonstrate a significant improvement in terms of dynamic flexibility. As IoT settings are dynamic and devices can join or leave the network at any time, the protocol is made to maintain and update group keys dynamically.
- Provide a comprehensive evaluation and validation of the proposed protocol. Its efficacy is evaluated through experimentation and simulation, considering factors, such as group key dissemination latency, memory overhead, and overall system performance.

II. RELATED WORKS

In [21], an effective method was presented to manage group keys in smart grid networks. In smart grids, photovoltaic facilities have cooperative groups of smart inverters that communicate over multiplex. However, smart grids did not offer a way to restrict who can view multicast data to authorized users. This study proposed a Key Management Service (KMS) to create and disseminate group keys, offering frequent renewal and confidentiality. This study tested a working prototype in a cluster of smart inverters and evaluated its efficacy. In MANETs, managing a collective key among a dynamic collection of nodes presents a challenge because users frequently forget to rekey or refresh the group key [22]. To enable the dynamic rekeying process in MANETs, a genetically based group key agreement strategy was proposed as a distributed group key management and broadcast stateless framework. The rekeying method establishes group keys employing Lagrange interpolation polynomial application over a finite region and hash functions. Additionally, a revocation system was provided to collect an exact rate of node misbehaviors to provide a robust security mechanism. In [23], key management mechanisms for data security-based transport in MANETs were proposed. This mechanism uses two specialized servers, the Distribution Key (DK) asymmetric key and the Calculator Key (CK) encryption. These two servers handle secret key creation, identification, and dissemination. Thus, no additional computation is required on other nodes to create the secret keys. These nodes are chosen based on their energy usage and node confidence ratings. In [24], a mutually verified GKM algorithm was presented for IoT healthcare systems. The proposed Mutually Authenticated Group Key Management Protocol (MAGKMP) enables an IoT device to successfully identify itself before becoming part of the network. In addition, it allows IoT devices to identify with reliable servers and intelligent e-health gateways before accessing session and group credentials. Following reciprocal verification between the various network participants' participating devices, group keys are safely disseminated for secure multicast communication. This study demonstrated that MAGKMP offers reciprocal authentication and forward and backward confidentiality in group communication, and it is safe against various attacks.

In [25], a GKM system was proposed to improve the effectiveness and convenience of healthcare IoT administration, combining elliptic curve encryption with one-way accumulation for sharing secret messages. This method updated the previously generated GK as the group's membership grew or shrank using classical ciphers, reducing processing and transmission costs. In [26], a hybrid secure routing protocol that inherits characteristics of both Ad-Hoc On-Demand Multipath Distance Vector (AOMDV) and multipath Optimized Link State Routing (OLSR) protocols was introduced. The recommended protocol provides multi-variant tuples based on the Two-Fish (TF) symmetric key technique to detect and eliminate adversaries in the global sensor network to deliver flexible protection. The eligibility weight function was combined with a complex symmetric key approach to select and hide sensor guard devices. In [27], a Trusted Secure Geographic Routing Protocol (TSGRP) for MANETs was suggested to provide safe and effective communication between nodes. This study considered the trust value for a node obtained by integrating direct and geographically trusted information to identify hackers. The source and destination nodes establish a secure trust-based communication channel. Following the sending of route-request and route-reply packets, the determined direct trust value is employed to determine the direct trust value of every node and an encrypted connection is created between the source and the destination network.

Since there are fewer sensor nodes available in WSNs than in conventional networks, privacy methods change [28]. Larger key sizes are necessary for current encryption systems to offer high-security levels, increasing the computing and interpersonal expenses associated with key formation. In [28], a hybrid key administration method was proposed for WSNs connecting devices at the edge that create pre-distribution keys

using elliptic curve cryptography and a hash function. The only requirement to obtain a key is to publish the node identity. To provide mutual authorization among the sensor nodes throughout the setup phase, an alternative key pre-distribution is mostly deployed. The proposed technique decreases computing difficulty while providing greater safety with limited resources. In [29], a dynamic cluster router protocol was proposed for IoT devices, following a neuro-fuzzy approach. This protocol builds dynamic clustering in a system utilizing an evolving self-organized neural network. Actual time events and cluster sensor nodes were identified using TinyOS. Simulation results disclosed that this protocol outperformed renowned green communications routing methods like Low-energy Adaptive Clusters Hierarchical and Low-energy Adaptive Clustered Hierarchical-Centralized by a large margin. The findings revealed that neuro-fuzzy logic is useful for applications such as green smart cities and sustainable IoT devices to handle resources and dynamic groupings.

The widespread use of IoT devices has led to numerous smart applications in various industries, including smart homes, wearable technology, education, agriculture, medical care, transportation, and many more [30]. As there are so many potential threats, the security of IoT devices remains a difficult problem. Therefore, strong security standards are a major concern to protect IoT smart devices [31-33]. A sensor network must choose an effective encryption technology to ensure secure transmission between its nodes. The creation and distribution of keys are fundamental prerequisites for encrypted communication. The key management process that is currently in use has a high computing overhead, consumes a lot of energy, and is slow. In addition, the limited available bandwidth of the sensing nodes renders the network inefficient.

III. PROBLEM STATEMENT

This study aims to tackle the security issues and vulnerabilities that IoT systems encounter in the area of routing protocols. Current IoT routing protocols are often weak and vulnerable to several security risks. This study intends to improve the security of communication within IoT systems by creating a unique, robust, and secure routing protocol that employs sophisticated group key management mechanisms. In the context of the dynamic and resource-constrained nature of IoT environments, the specific issues addressed include the need for resilience against attacks, effective management of cryptographic keys within groups of devices, and the general establishment of a secure and reliable communication framework. By tackling these obstacles, this study aspires to help create safe and effective routing protocols adapted to the particular characteristics of IoT systems [34].

IV. THE PROPOSED ROUTING PROTOCOL BASED ON GKM

The proposed approach deals with security issues in IoT. GKM is one of the most important techniques for delivering safe data in dynamic IoT situations. The DLGKM framework was proposed to deal with the scaling problems and inefficiencies of the existing GKM models. The system seeks to achieve faster and more efficient multicast message delivery when integrated with a REMI-DLGKM. Compared to modern protocols, such as SRPL, QMR, and MAODV, the proposed one performs better in the Cooja Simulator in terms of end-to-end latency, energy usage, and packet delivery ratio. This indicates that the suggested routing protocol can be exploited to reduce IoT device energy consumption by using following key management techniques.

A. Routing Protocol

The REMI cluster-based multiplex protocol employs the RPL MOP 3 mode for optimization. This method is used to spread messages throughout an IoT network. At first, before data transfer between nodes, REMI deploys Destination Oriented Directed Acyclic Graph (DODAG) and cluster creation. In the next stage, it transmits data. A producer node must transmit a multiplex message in three different directions, implementing the REMI protocol in an RPL DODAG tree: (i) upward to its initial node, (ii) downward to any prospective children who have joined the mesh network, and (iii) to the neighbors of various cluster IDs. When a data packet has numerous neighbors within a single cluster, the message is only delivered to just one of them, since if any network node has a message, it distributes it throughout the entire cluster. Two distinctive cases are described in the following sections: when the originator node is and when it is not the DODAG root.

1) The Originator or Transmitting Node is the DODAG Root

If the provider is the DODAG root, all its children will receive the message. Roots will first examine their routing information to deliver the multiplex packet downwards to only the children connected to this broadcast group. However, if the roots have no offspring, they will discard the message. The root node initially sets a header option called C2C to 1 in IPv6 while transmitting them to its relevant children [30]. The packets are then sent to the youth using an efficient routing mechanism. The OFM provides a sufficient trade-off between the number of broadcasts and copies in the system. If or less than half of the producer node's entire number of kids are engaged in the packet header, a producer node implementing OFM will perform a connectionless relaying to them. The reduction in communication transmission, which might be more successful if there are many engaged kids, reduces the number of repetitions in the system. The C2C is included in the header because if the root node forwards a message, all clusters will get it almost simultaneously. This results from the cluster members being the root node's offspring.

Another instance involving the root is when it receives a multiplex target message that needs to be forwarded. The base first saves the contents of the packet received and the network ID that the packet was received in a special database called the Discard Duplicated Forward (DDF) table. It also attaches a brief timer to each update in the database. Once the timer runs out, the root collects data for all the copies of this packet. The major reason for utilizing this duration is to prevent the root's replication from spreading throughout the clusters. Whenever the game ends, the root looks for the node IDs linked with this message in its DDF table. Since these nodes have already analyzed the packet on their way back to the root, the root would not send it to them.

There could be a limited message size allowed by the protocol. When a received message exceeds this threshold, it may be rejected since it may be a sign of a possible protocol infraction or the existence of inaccurate data. The message can be refused to stop unauthorized or compromised communication if it contains measures for authentication or security, such as digital signatures or encryption, and these mechanisms fail to authenticate or decode the message.

2) The Originator or Transmitting Node is a Non-Root Node

When a non-root node transmits data as an origin or as a forwarder, it sends the packet over a link along the upward manner to its member nodes, in the horizontal position to the engaged pupils, and to its neighborhood, who are members of a different cluster. These neighborhoods use the affiliated cluster ID with every neighborhood node ID. A relaying router will randomly deliver the packets to one neighborhood if it finds numerous neighborhoods that share the same cluster ID in the neighboring set. When transmitting an IPv6 message with a multiplex default gateway, a node first examines the Duplicate Detection Table (DDT) to prevent handling identical packets. If the delivery is flagged as duplication, the node discards it. A recommended provider sends a packet following the next steps:

- Step 1: The node processes the incoming message to determine the C2C *ag* state. If *ag* is not set, the node can transmit messages to its neighboring nodes or a different cluster member. In the other case, the node proceeds to Step 2.
- Step 2: If any relevant children are enrolled for the multiplex address in the incoming message, the node examines its forwarding table before forwarding the message to them via OFM. If not, the node moves to Step 3.
- Step 3: Determine whether the incoming message's multicast group includes the node directly. If so, the node should transmit the message to the core network. Otherwise, it should reject it.

Receiving a package from a neighborhood:

- Step 4: Node transmits the message to its desired parent.
- Step 5: Node completes steps 1, 2, and 3.

B. Proposed Group Key Management

Decentralized Lightweight Group Key Management (DLGKM) has three fundamental layers. Devices and users are defined by the top and bottom levels, respectively. The decentralized manager, or KDC, is defined in the inner layer and manages the keys between both inside groups. Figure 2 illustrates the architecture of the proposed DLGKM.

1) Device Groups

DLGKM establishes a predetermined number of Device Groups (DGs) for the IoT context depending on their functionality, system security, localization, etc. A new IoT device that enters the network is excessively focused on one of the active DGs. Inside a DG, the Logic Key Hierarchy (LKH) system permits information sharing.

2) User Groups

DLGKM develops user groups according to user interests and duration of registrations. Each client enters any of these User Groups (UGs), and then the private keys are transferred inside each UG.

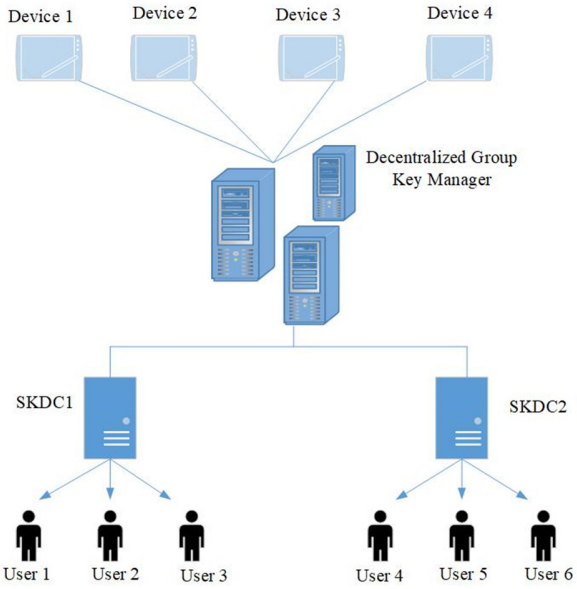

Fig. 2. Architecture of the proposed DLGKM.

ALGORITHM 1: GKM ALGORITHM

Step1: Initialization
Generate a random group key called K.
Create a secure channel of communication between the group members and the group key server.
Step2: Key Distribution
Safely keep the group key K and keep track of the public keys of each member of the group.
Create a special pair of public and private keys (PK, SK) and submit the public key PK for registration to the GKS.
Obtain the group member's public key PK, and add it to the list.
Step3: Key Updates
Start a key update procedure periodically or on demand.
Create a group key K_{new} which is encrypted by the public keys of each group keys.
Send to each group member the encrypted key K_{new}.
When receiving K_{new}, each member decrypts this key using its private key.
Keep the group key K_{new} on its memory.
Step4: Group Communication
Now, group members may securely communicate with each other by using the shared group key K or K_{new}.
Step5: Key Revocation
Remove the member from the group list if membership in the group has to be canceled. Then, make a fresh group key called $K_{revocation}$.
Use the public keys of all remaining group members to encrypt $K_{revocation}$, which is sent to each group member.
When receiving $K_{revocation}$, each member decrypts this key using its private key
Revoked group key $K_{revocation}$ should be kept in a safe place. Don't communicate further using $K_{revocation}$.

V. DECENTRALIZED GROUP KEY MANAGER

A KDC and several SKDCs comprise the decentralized application server for IoT environments [36]. The requirements of IoT applications determine the amount of SKDC, which is not a set. More precisely, SKDC attributes such as memory, processing power, and active users affect its total amount. The KDC is the main server that transmits messages to the rest of the network and controls how the DGs renew their keys. Moreover, KDC has a data backup that keeps track of the most recent updates to the device's keys, which are regularly delivered after many processes. Also, SKDCs oversee the UGs' information sharing, where individuals constantly enter and exit the network. As a result, the decentralized nature of the controllers, which use SKDCs, enables reducing the burden on the KDC. According to a localized user, different user organizations have the authority of the same SKDC, eliminating the issue of SKDC failure and guaranteeing the platform's sustainability. Additionally, the decentralized KDC can create a one-time encrypted connection with members and devices that may be deployed to identify and establish a new member user or a device before disclosing the encrypted information to them. The GKM is divided into five steps, as observed in Algorithm 1.These steps are repeated as needed for periodic key updates and revocations.

A. Requirements of Group Key Management

GKM is a process for securely establishing, distributing, updating, and revoking encryption keys inside a group or multicast communication environment [35]. The basic goal of group key management is to ensure that only authorized group members can access the shared encryption key, allowing secure communication while preserving the privacy and integrity of group messages. It is more difficult to handle keys in group communication situations than in P2P communication, as there are more participants and the key needs to be securely given to all authorized group members in group communication situations than in P2P communication. For efficient GKM, several prerequisites are recognized and clarified. In theory, an effective and realistic GKM must consider the following criteria.

1) Security Requirements

The network must perform some functions in a dynamic IoT context to ensure communicated data protection. To guarantee forward secrecy, this should prevent any departing participant from decoding any network-based transmission. On the other hand, to ensure backward secrecy, active arrivals that enter the network must be blocked from decoding the earlier conversations. Oriented secrecy can be achieved with an effective key-upgrading procedure. All keys must be entirely separate to protect them independently.

2) Effective Functioning Requirements

The minimal manufacturing overhead of various measurements justifies the effective operation of important managerial procedures. The first benefit is lower storage overhead, as fewer keys are saved on people and IoT devices. Second, it eliminates the computing power needed by people, IoT devices, and computers, improving capacity by reducing time. Ultimately, it decreases the volume of information transferred on the network, increasing adaptability, and reducing transaction costs.

3) Performance Requirements

Performance is mainly influenced by elements that affect group interaction. Durability is a component that establishes the capacity to deal with varying group sizes and significant fluctuations in participation. The 1-impacts-n phenomenon, where one server's breakdown results in the entire system's breakdown, also affects key management techniques. As a result, it is crucial to prevent this problem and guarantee reliability in a big, scalable network.

VI. RESULTS AND DISCUSSION

This section examines how changes in the target network's subscriber percentage affect the different networking parameters used by the REMI-DLGKM routing protocol. Extensive simulations were performed in the Cooja simulator [36] to evaluate the proposed protocol. Some networking factors, including packet delivery ratio, end-to-end latency, and energy usage, were considered to evaluate its performance. The proportion of sink nodes varies between 20 and 80%. In the simulation, the nodes can move by the Two Ray Ground model in a 1000×1000 m area for 1000 s. The simulation was carried out by randomly choosing 10 nodes to act as wormhole nodes to evaluate the impact of wormhole assaults on the system's Packet Delivery Ratio (PDR). Suppose that the DODAG is protected from wormhole assaults. In that case, it should also be protected from other attacks with a similar single point of routing disruption, such as sink-hole, black-hole, and selective-forwarding attacks.

A communication model that specifies how messages are exchanged between group members and the GKS was implemented in the simulation environment to evaluate the algorithm's behavior and effectiveness. The results shown in Tables I, II, and III are subject to different experimental or simulated settings that are particular to the assessment of the corresponding algorithms. The different cases include node density, traffic patterns, network structure, and communication paradigms.

A. Packet Delivery Ratio (PDR)

PDR indicates the proportion of packages sent to clients by the application layer sources to the entire packets the subscribers received at their destination.

$$PDR = \frac{\sum Number\ of\ packets\ received}{\sum Number\ of\ packets\ send} \quad (1)$$

The purpose of a wormhole attack is to transfer the data from a compromised node to a malicious one through a tunnel. Thus, other nodes in the network believe that they are closer to other nodes, which can cause problems in the routing algorithm. Besides, the compromised nodes can manipulate the packet. Table I portrays the impact of PDR during the wormhole attack. Figure 3 reveals that the PDR of the proposed algorithm outperformed the SRPL and QMR protocols. This is because the communication in REMI-DLGKM is secured by secret keys (public and private keys). The probability that a node in the network is compromised is very low as the nodes can perform a mutual authentication. Thus, no problem can

occur in the routing process, and the PDR is higher. With a 99.21% PDR, REMI-DLGKM significantly outperformed SRPL, QMR, and MAODV. The compromised nodes in these algorithms caused by the wormhole attack can isolate part of the network and hence affect PDR.

TABLE I. IMPACT OF PDR DURING WORMHOLE ATTACK

Protocol	Packet delivery ratio (PDR) (%)
SRPL	99
QMR	96.10
MAODV	90
REMI-DLGKM	99.21

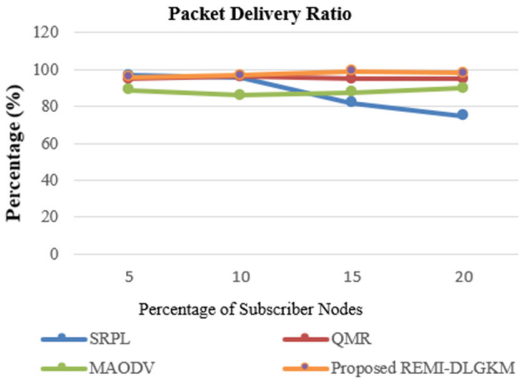

Fig. 3. Network PDR impact during a wormhole attack with a high number of subscribers.

B. Energy Consumption

Energy consumption in the context of GKM refers to the amount of electrical power used by devices engaged in key management operations inside a group or multicast communication situation. It particularly focuses on the energy consumption connected to the creation, distribution, modification, and revocation of encryption keys among a group. Figure 4 depicts the energy consumption per packet that is effectively transported to its destination.

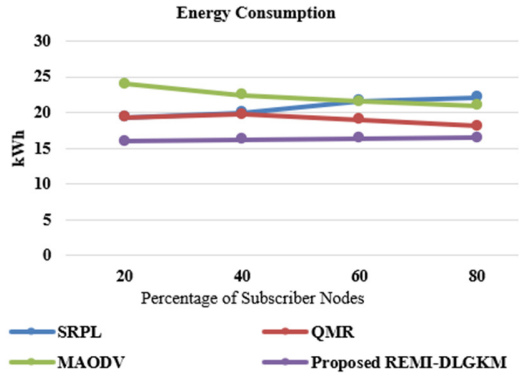

Fig. 4. Energy consumption per packet that is successfully delivered to its destination with an increasing number of subscriber nodes.

REMI-DLGKM has a lower energy consumption than other protocols because it requires fewer transactions to transmit a multiplex message to all its destinations. The proposed GKM scheme is not complex like the hash chain technique used in SRPL, hence the nodes do not need to consume more energy when executing it. In addition, in REMI-DLGKM, if a device receives a packet, it does not need to forward it to all nodes in the cluster, but it sends it only to the cluster head as a cluster creation takes place. Moreover, no additional computation is required on ordinary nodes to create the group key, as it is created by the GKS. This leads to reduced energy consumption.

TABLE II. COMPARISON OF ENERGY CONSUMPTION

Methods	Energy consumption (kWh)
SRPL	19.32
QMR	18.12
MAODV	21.99
Proposed REMI-DLGKM	16

C. End-to-End Delay

In a communication network, the end-to-end delay shows how long it takes a packet to travel from its source to its destination. This delay includes all of the communication process's components, such as processing, queuing, propagation, and transmission delays. Table III compares the communication latency performance of SRPL, QMR, MAODV, and the proposed REMI-DLGKM. In general, a more responsive and efficient network has a reduced end-to-end delay. With the lowest end-to-end delay of 0.6 s in this context, the proposed REMI-DLGKM stands out and can be more responsive than SRPL (1.09 s) and QMR (1.22 s). Additionally, MAODV exhibits competitive performance with a 0.8 s end-to-end delay. In networking contexts, communication latency can be minimized by using the REMI-DLGKM routing protocol. This is because the proposed technique of GKM is not complex, so each node does not need more time to encrypt or decrypt the received packet. This is especially important for applications that need to respond quickly, such as multimedia streaming or interactive communication. Figure 5 exhibits a comparison of end-to-end delays between algorithms.

TABLE III. COMPARISON OF END-TO-END DELAY

Method	End-to-end delay (s)
SRPL	1.09
QMR	1.22
MAODV	0.8
Proposed REMI-DLGKM	0.6

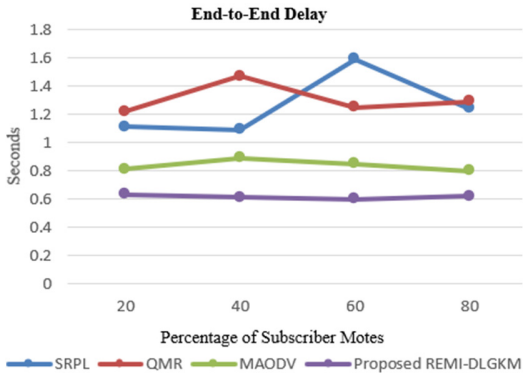

Fig. 5. End-to-end delay comparison between algorithms.

VII. CONCLUSION AND FUTURE SCOPE

Although IoT offers new opportunities, safety is always a top concern while providing a variety of amenities. It is especially difficult to protect IoT device-generated information against security threats and to secure its exchange as it travels through numerous nodes and gateways. Therefore, in these dynamic scenarios, GKM can control the distribution of keys for internet connectivity and secure data transmission. However, the huge number of IoT devices and the growing subscriber base offer a scalability issue, which is not solved by the existing GKM-based IoT-specific verification solutions. Furthermore, every one of the GKM models in use today supports individual independence. Every subdivision exclusively focuses on dependent symmetrical group keys, which are inadequate for subscriptions with extremely dynamic behavior. To solve these problems, an innovative DLGKM architecture for network access is needed in IoT applications. This study introduced REMI-DLGKM, a reliable and effective multiplex routing solution for IoT networks, which uses cluster-based routing technology to speed up the system's multiplex message communication. The simulation results disclosed that the proposed protocol outperformed the existing ones in end-to-end delay, energy use, memory utilization, and PDR. Future research will focus on methods to prevent more targeted and all-encompassing attacks on routing protocols in IoT networks.

ACKNOWLEDGEMENTS

The authors gratefully acknowledge the approval and support of this research study by grant no CSAT-2022-11-1539 from the Deanship of Scientific Research at Northern Border University, Arar, K.S.A.

REFERENCES

[1] Y. B. Zikria, M. K. Afzal, F. Ishmanov, S. W. Kim, and H. Yu, "A survey on routing protocols supported by the Contiki Internet of things operating system," *Future Generation Computer Systems*, vol. 82, pp. 200–219, May 2018, https://doi.org/10.1016/j.future.2017.12.045.

[2] L. Wu, X. Du, W. Wang, and B. Lin, "An Out-of-band Authentication Scheme for Internet of Things Using Blockchain Technology," in *2018 International Conference on Computing, Networking and Communications (ICNC)*, Maui, HI, USA, Mar. 2018, pp. 769–773, https://doi.org/10.1109/ICCNC.2018.8390280.

[3] S. Anamalamudi, A. R. Sangi, M. Alkatheiri, and A. M. Ahmed, "AODV routing protocol for Cognitive radio access based Internet of Things (IoT)," *Future Generation Computer Systems*, vol. 83, pp. 228–238, Jun. 2018, https://doi.org/10.1016/j.future.2017.12.060.

[4] Z. Mahmood, A. Ullah, and H. Ning, "Distributed Multiparty Key Management for Efficient Authentication in the Internet of Things," *IEEE Access*, vol. 6, pp. 29460–29473, 2018, https://doi.org/10.1109/ACCESS.2018.2840131.

[5] H. Gu and M. Potkonjak, "Efficient and Secure Group Key Management in IoT using Multistage Interconnected PUF," in *Proceedings of the International Symposium on Low Power Electronics and Design*, Seattle, WA, USA, Apr. 2018, https://doi.org/10.1145/3218603.3218646.

[6] A. M. Rahmani *et al.*, "Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach," *Future Generation Computer Systems*, vol. 78, pp. 641–658, Jan. 2018, https://doi.org/10.1016/j.future.2017.02.014.

[7] A. Čolaković and M. Hadžialić, "Internet of Things (IoT): A review of enabling technologies, challenges, and open research issues," *Computer Networks*, vol. 144, pp. 17–39, Oct. 2018, https://doi.org/10.1016/j.comnet.2018.07.017.

[8] Y. B. Zikria, H. Yu, M. K. Afzal, M. H. Rehmani, and O. Hahm, "Internet of Things (IoT): Operating System, Applications and Protocols Design, and Validation Techniques," *Future Generation Computer Systems*, vol. 88, pp. 699–706, Nov. 2018, https://doi.org/10.1016/j.future.2018.07.058.

[9] A. Triantafyllou, P. Sarigiannidis, and T. D. Lagkas, "Network Protocols, Schemes, and Mechanisms for Internet of Things (IoT): Features, Open Challenges, and Trends," *Wireless Communications and Mobile Computing*, vol. 2018, Sep. 2018, Art. no. e5349894, https://doi.org/10.1155/2018/5349894.

[10] W. Sun, Z. Cai, Y. Li, F. Liu, S. Fang, and G. Wang, "Security and Privacy in the Medical Internet of Things: A Review," *Security and Communication Networks*, vol. 2018, Mar. 2018, Art. no. e5978636, https://doi.org/10.1155/2018/5978636.

[11] Y. Cui, Y. Ma, Z. Zhao, Y. Li, W. Liu, and W. Shu, "Research on data fusion algorithm and anti-collision algorithm based on internet of things," *Future Generation Computer Systems*, vol. 85, pp. 107–115, Aug. 2018, https://doi.org/10.1016/j.future.2018.03.016.

[12] S. Belhaj and S. Hamad, "Routing protocols from wireless sensor networks to the internet of things: An overview," *International Journal of Advanced and Applied Sciences*, vol. 5, no. 9, pp. 47–63, Sep. 2018, https://doi.org/10.21833/ijaas.2018.09.009.

[13] L. Tello-Oquendo, I. F. Akyildiz, S.-C. Lin, and V. Pla, "SDN-based architecture for providing reliable Internet of Things connectivity in 5G systems," in *2018 17th Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net)*, Capri, Italy, Jun. 2018, https://doi.org/10.23919/MedHocNet.2018.8407080.

[14] V. Adat and B. B. Gupta, "Security in Internet of Things: issues, challenges, taxonomy, and architecture," *Telecommunication Systems*, vol. 67, no. 3, pp. 423–441, Mar. 2018, https://doi.org/10.1007/s11235-017-0345-9.

[15] M. Conti, P. Kaliyar, M. M. Rabbani, and S. Ranise, "SPLIT: A Secure and Scalable RPL routing protocol for Internet of Things," in *2018 14th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, Oct. 2018, pp. 1–8, https://doi.org/10.1109/WiMOB.2018.8589115.

[16] J. Karlsson, L. S. Dooley, and G. Pulkkis, "Secure Routing for MANET Connected Internet of Things Systems," in *2018 IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud)*, Barcelona, Spain, Aug. 2018, pp. 114–119, https://doi.org/10.1109/FiCloud.2018.00024.

[17] Z. A. Almusaylim, N. Z. Jhanjhi, and A. Alhumam, "Detection and Mitigation of RPL Rank and Version Number Attacks in the Internet of Things: SRPL-RP," *Sensors*, vol. 20, no. 21, Jan. 2020, Art. no. 5997, https://doi.org/10.3390/s20215997.

[18] J. Liu *et al.*, "QMR:Q-learning based Multi-objective optimization Routing protocol for Flying Ad Hoc Networks," *Computer Communications*, vol. 150, pp. 304–316, Jan. 2020, https://doi.org/10.1016/j.comcom.2019.11.011.

[19] D. M. Babu and M. Ussenaiah, "CS-MAODV: Cuckoo search and M-tree-based multiconstraint optimal Multicast Ad hoc On-demand Distance Vector Routing Protocol for MANETs," *International Journal of Communication Systems*, vol. 33, no. 16, 2020, Art. no. e4411, https://doi.org/10.1002/dac.4411.

[20] G. Manikandan and U. Sakthi, "A Comprehensive Survey on Various key Management Schemes in WSN," in 2018 2nd International Conference on 2018 2nd International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, India, Aug. 2018, pp. 378–383, https://doi.org/10.1109/I-SMAC.2018.8653656.

[21] M. Basile, G. Dini, F. Vernia, and L. Lamoglie, "A Secure and Efficient Group Key Management Scheme for Clusters of String Inverters," *Applied Sciences*, vol. 10, no. 21, Jan. 2020, Art. no. 7900, https://doi.org/10.3390/app10217900.

[22] V. S. Janani and M. S. K. Manikandan, "An Efficient Genetic Based Broadcast Stateless Group Key Management Scheme with Dynamic Rekeying in Mobile Ad-Hoc Networks," *Wireless Personal Communications*, vol. 105, no. 3, pp. 857–876, Apr. 2019, https://doi.org/10.1007/s11277-019-06125-3.

[23] P. Bondada, D. Samanta, M. Kaur, and H.-N. Lee, "Data Security-Based Routing in MANETs Using Key Management Mechanism," *Applied Sciences*, vol. 12, no. 3, Jan. 2022, Art. no. 1041, https://doi.org/10.3390/app12031041.

[24] F. Kausar, W. Aman, and D. Al-Abri, "Mutually Authenticated Group Key Management Protocol for Healthcare IoT Networks," in *Proceedings of the Future Technologies Conference (FTC) 2019*, 2020, https://doi.org/10.1007/978-3-030-32523-7_1.

[25] C. Trivedi and U. P. Rao, "Secrecy aware key management scheme for Internet of Healthcare Things," *The Journal of Supercomputing*, vol. 79, no. 11, pp. 12492–12522, Jul. 2023, https://doi.org/10.1007/s11227-023-05144-z.

[26] B. D. Deebak and F. Al-Turjman, "A hybrid secure routing and monitoring mechanism in IoT-based wireless sensor networks," *Ad Hoc Networks*, vol. 97, Feb. 2020, Art. no. 102022, https://doi.org/10.1016/j.adhoc.2019.102022.

[27] F. H. Shajin and P. Rajesh, "Trusted Secure Geographic Routing Protocol: outsider attack detection in mobile ad hoc networks by adopting trusted secure geographic routing protocol," *International Journal of Pervasive Computing and Communications*, vol. 18, no. 5, pp. 603–621, Jan. 2020, https://doi.org/10.1108/IJPCC-09-2020-0136.

[28] Sharmila, P. Kumar, S. Bhushan, M. Kumar, and M. Alazab, "Secure Key Management and Mutual Authentication Protocol for Wireless Sensor Network by Linking Edge Devices using Hybrid Approach," *Wireless Personal Communications*, vol. 130, no. 4, pp. 2935–2957, Jun. 2023, https://doi.org/10.1007/s11277-023-10410-7.

[29] P. Chithaluru, F. Al-Turjman, M. Kumar, and T. Stephan, "Energy-balanced neuro-fuzzy dynamic clustering scheme for green & sustainable IoT based smart cities," *Sustainable Cities and Society*, vol. 90, Mar. 2023, Art. no. 104366, https://doi.org/10.1016/j.scs.2022.104366.

[30] A. B. Feroz Khan and G. Anandharaj, "AHKM: An improved class of hash based key management mechanism with combined solution for single hop and multi hop nodes in IoT," *Egyptian Informatics Journal*, vol. 22, no. 2, pp. 119–124, Jul. 2021, https://doi.org/10.1016/j.eij.2020.05.004.

[31] N. A. Alsharif, S. Mishra, and M. Alshehri, "IDS in IoT using Machine Learning and Blockchain," *Engineering, Technology & Applied Science Research*, vol. 13, no. 4, pp. 11197–11203, Aug. 2023, https://doi.org/10.48084/etasr.5992.

[32] A. O. Aljahdali, A. Habibullah, and H. Aljohani, "Efficient and Secure Access Control for IoT-based Environmental Monitoring," *Engineering, Technology & Applied Science Research*, vol. 13, no. 5, pp. 11807–11815, Oct. 2023, https://doi.org/10.48084/etasr.6193.

[33] S. A. Alshaya, "IoT Device Identification and Cybersecurity: Advancements, Challenges, and an LSTM-MLP Solution," *Engineering, Technology & Applied Science Research*, vol. 13, no. 6, pp. 11992–12000, Dec. 2023, https://doi.org/10.48084/etasr.6295.

[34] M. Dammak, S. M. Senouci, M. A. Messous, M. H. Elhdhili, and C. Gransart, "Decentralized Lightweight Group Key Management for Dynamic Access Control in IoT Environments," *IEEE Transactions on Network and Service Management*, vol. 17, no. 3, pp. 1742–1757, Sep. 2020, https://doi.org/10.1109/TNSM.2020.3002957.

[35] Y. Baddi, S. Anass, K. Zkik, Y. Maleh, B. Mohammed, and E.-C. El Kettani Mohamed Dafir, "MSDN-GKM: Software Defined Networks Based Solution for Multicast Transmission with Group Key Management," in *Machine Intelligence and Big Data Analytics for Cybersecurity Applications*, Y. Maleh, M. Shojafar, M. Alazab, and Y. Baddi, Eds. Cham, Switzerland: Springer International Publishing, 2021, pp. 373–396.

[36] "Contiki Cooja Simulator : Specially Designed Wireless Sensor Networks," *Ns3 Projects*. https://ns3simulation.com/contiki-cooja-simulator/.