International Journal of Innovative Technology and Interdisciplinary Sciences
https://journals.tultech.eu/index.php/ijitis
ISSN: 2613-7305
Volume 8, Issue 3
DOI: https://doi.org/10.15157/IJITIS.2025.8.3.496-512
Received: 29.07.2025; Revised: 19.08.2025; Accepted: 26.08.2025

Research Article

SCP-IoT: Enhancing IoT Communication Security Against Routing Attacks

L.K. Suresh Kumar[1], Venkat Dass Maredu[1], Rasineni Madana Mohana[2], Palamakula Ramesh Babu[3], Kadiyala Ramana[4,*]

[1] Department of Computer Science and Engineering, Osmania University, Hyderabad, Telangana, India.

[2] Department of Computer Science and Engineering, Stanley College of Engineering & Technology for Women, Hyderabad, Telangana, India.

[3] Department of Information Technology, Chaitanya Bharathi Institute of Technology, Hyderabad, Telangana, India.

[4] Department of Artificial Intelligence and Data Science, Chaitanya Bharathi Institute of Technology, Hyderabad, Telangana, India.

***ramana.it01@gmail.com**

Abstract

The Internet of Things (IoT) needs to be protected while in transmission. Insecure Internet of Things equipment connectivity can direct to security breaches. As a result, third parties can get access and make changes in order to cause problems for things connected in the system. In order to address these difficulties, the IoT communication security needs to be addressed. A new strategy named "secure communication utilising cryptographic approaches for IoT" was presented in this research to deal with this problem. There are three parts to the model, which is called the "safe communication protocol for IoT." First, the initiator sends a connection request to the respondent with the source identification and a true cryptography nonce to initiate the communication. Secondly, the responder examines the nonce's freshness and the source's identity when it receives a request. After that, the responder uses KDH to compute and deliver the MAC result for the SRC ID as part of the Finish message to the initiator. Few current strategies, including developing constrain fuzzy routing principles, were evaluated and compared to the proposed model. Prior to this study, the most important metrics were the MLR and MDR ratios, the spectrum utilisation rate, the network lifetime, and the utilisation rate.

Keywords: Connectivity; Message integrity; Internet of Things (IoT); Cryptography.

INTRODUCTION

IoT refers to a network in which a large number of things are linked together. By being (1) online or structural, (2) independent in its decision-making and functioning; (3) connected; (4) interoperable; (5) flexible in its ability to interact with other item at anytime, anywhere, and for any service; and (6) autonomous in its ability to make its own decisions.

[1]. As a result, the Internet of Things (IoT) is not one technology, but rather a collection of many, including Sensor Network (WSN), Radio Frequency (RFID), Intelligent Ad Hoc Networks (SANET), Connectivity Fidelity networks (WIFI), Wireless Body Area Network (WPAN), and many more. As a result, today's Internet of Things (IoT) is an enormously diverse network [2-5].

When it comes to IoT connectivity, there are a plethora of protocols and ways to choose from. Ad hoc mode is one of the most popular options [4, 6]. ad hoc networks are peer-to-peer (p2p) networks without a permanent infrastructure in which every device gather, analyses and transmits data on its own [7]. There are direct wireless transmissions between devices, as well as multi-hop transmissions for nodes outside the radio transmission area. To increase the range of its own transmission, a transmitting object employs other items as relays in the multihop situation. As a result, establishing routes and forwarding packets to their targets is delegated to intermediary objects by a device. Many advantages can be gained by employing ad-hoc networks, such as quick deployment, lower costs, and support with mobility. IoT applications involving disaster relief, collaborative Vehicles with advanced driver assistance systems, electronic health records (EHRs), supply chains, the military, and environmental sensing all make heavy use of ad hoc connectivity [8]. A key component of 5G deployment is the ability to scale the network's coverage while also assuring the services' robustness and providing a better user experience via ad hoc mode [9-11].

Attacks on IoT systems are increasing in quantity and sophistication as the sector develops [12]. An IoT system attack is one that aims to get access to sensitive data, add bogus data, or disrupt services. [13]. Smart refrigerators, medical gadgets, & smart cars have all been targeted in recent hacks [14]. It is possible that some attacks, such as hacking medical devices, could result in the deaths of people. As a result, protecting key IoT systems from malicious assaults and failures is a top priority.

Privacy protection, consistency, and accessibility are all part of what we mean when we talk about information security. According to Schneider, attacks on availability and integrity are more critical than assaults on confidentiality in the Web of Things [14]. In the same way, preventing an intruder from operating your car is more vital than protecting your whereabouts from being eavesdropped on. It is extremely difficult to keep hackers from taking over an IoT system.

Limitations

Most of the models that have been suggested do not consider dynamic topology, driving directions, mobility characteristics, or energy considerations. When a network is overloaded with broadcast messages-based classification in the initial phases, collisions are more likely to happen.

Motivation

The proposed approach is designed to deal with the challenges that are raised during the communication process. This problem necessitates the use of light-weight concepts for secure communication. Reliability is improved using a strategy cryptography - Based, which has proven to be the most efficient.

The main contributions of this paper are as follows:

- We propose a novel Secure Communication Protocol (SCP) integrating distributed Key Derivation using Hybrid Diffie–Hellman (KDH) and proxy-assisted message forwarding to enhance routing security in IoT networks.
- SCP is explicitly designed to operate under adversarial conditions including replay and spoofing attacks, with minimal performance degradation.
- We provide complete reproducibility with NS-3.35 simulation configurations, attack scenarios, and cryptographic settings.
- We conduct comparative performance evaluation against EPFR, ESLP-IoT, and HiLSeR under both normal and attack conditions, showing improvements in message delivery ratio (up to +12%), reduced latency (up to −35%), and lower routing overhead (up to −50%).
- We analyze scalability up to 1,000 nodes and quantify computational and energy costs for resource-constrained IoT devices.

The goal of this study is to use cryptographic principles to overcome communication challenges for IoT applications at the transmission and connection level. There are four sections in the paper: relevant work, model suggested, experimental setup, discussion of the findings and conclusion.

RELATED WORKS

IoT privacy is a major security concern that academics in industry and academia must address head-on. IoT privacy mechanisms and management frameworks are urgently needed [15, 16]. Internet of Things (IoT) has become an important aspect of many applications, including remote healthcare monitoring and energy usage control. User privacy is essential in each of these applications since it pertains to a user's whereabouts, behaviors, and contacts with other individuals.

There is now a lot of research done recently on the privacy and security of IoT in the cloud, such as [17]. Identification privacy, personal privacy, node compromise, layer removal/addition at once, forward backward security, and semi-trusted and malevolent cloud security are some of the privacy and security needs of IoT in the cloud, according to the authors of the paper [18] is another recent study that attempts to assess known privacy-preserving technologies. In their numerous recommendations, the authors found holes that needed to be filled and made suggestions for how to fill those gaps.

Surveys of current IoT applications were carried out by the authors in [19]. It was the authors' goal to translate their modules into a universal system model as well as to study differential behavioural patterns created by sensor data. It was discovered that practically all applications collect location information from the analysis. Video and audio are only two examples of the many data formats that can be used to store the information that is collected. The authors looked at the most recent privacy protections. It has also been suggested how user privacy can be threatened in participatory sensing by uncontrolled personal information to unauthorised parties. They then mapped their findings onto a model for examining safety in mobile participatory sensor applications that the authors had developed.

Security and privacy risks in IoT designs are discussed in depth in [20]. The first part of the lecture focuses on the IoT's multi-layered design. Security and privacy risks have been carefully looked at and written down at each and every stage of the architecture. In-depth research is done on the current state of the art when it comes to presenting hazard situations at various levels of the Architecture. The most essential security issues in the scenarios outline are eavesdropping, person attacks, and taking control of some components. The writers also look into to the new IoT laws in the EU. The administration regions of the IoT architecture must be known. Individuals in the EU are required by law to have full access to and control over their personal data at all layers of the information architecture. This kind of management necessitates deeper investigation into how it is technically provided. Research into privacy and security risks has to focus on the energy side of things.

Various privacy advancements in the Internet of Things (IoT) have been surveyed in [21]. We'll talk about some of the most important future security needs for smart homes. Additionally, the authors proposed an IoT security architecture. It has been suggested that the portal architecture is best suited for wealth devices and high system uptime. Using a moderately strong processor, this design can run key smart home functions. Besides gateways, alternative architectures for IoT include middleware and cloud architecture, respectively. System security is enhanced by the use of an auto-configuration tool, and automatic software and firmware updates are also mentioned for a gateway design to help with auto management.

In [22], an effort is made to manage security for IoT by means of IFC tags for efficient information tagging. Sensitive information is marked with confidentiality characteristics that let trusted controls decide who can see it based on how important it is. It costs a lot to tag an IoT device because it needs a lot of resources. This work talks about the problems with tagging energy IoT devices. For privacy-sensitive IoT applications, the IFC data tag is a viable solution due to its ability to protect the physical interaction, the sensing of valuable data, and the distributed implementation. In addition to these four, there really are two more aspects of these applications that enable deployment of IFC information tags much easier: connected operations and skewed tag utilisation.

It has been proposed in [23] that a Host Identification Protocol (HIP) with Multimedia Web Keying Protocol (MIKP) might be used to establish a secure alliance between the network and the host. Public key cryptography is used to identify IoT devices via HIP. As an added bonus, the authors of HIP have included tools for managing its various keys. MSNs need an competent & consistent security systems system which was critical to allowing staff access to confidential medical information and ensuring creative & reliable admission control for medical sensor networks (MSNs).

Authors at [24] has presented an access control that can be used in medical circumstances where access control is needed. The classic role-based access control concept is being extended in this new system. Access control decisions can be made more easily, and policies can be distributed more efficiently, with modular architecture.

In [25], the security of wireless sensing applications was examined by the authors. Nominated application scenarios were offered by the authors in order to highlight potential benefits derived from their use. Data flow and varied statistics collected by current wireless sensing applications were examined by researchers. Threats to one's privacy are given particular attention. Existing mobile sensing installations are under attack from these vulnerabilities, which target key data and sensor readings. Spatiotemporal information, sound sampling and images, videos and accelerometer data are included in these readings. Sensor data that has been annotated over time can reveal information about a user's personal behaviours, putting their privacy at risk, and the emergence of spatiotemporal readings poses a privacy risk in and of itself. In the absence of safeguards to protect user privacy, automated collection of sound samples creates major privacy hazards, as private conversations will be captured. Images & video put the confidentiality of other persons in the photographs taken by the customer at risk since they can betray their current location and the identities of social relations.

The authors of [26] classified methods to IoT as rule-based or architectural. Architecture-based privacy safeguards were proposed by the authors of this paper. Everything in the Internet of Things (IoT) works together as a team to achieve a common goal. IoT privacy protection is supported via the Contract Net Protocol (CNP).

According to [27], the most particular segment of IoT networks for privacy and security are available. Home automation networks, which the authors suggest can be expanded to include IoT applications, were the primary concern of the writers.

In [29], Zhang et al. presented a comprehensive study on integrating edge computing with IoT privacy frameworks, showing how distributed computation near the data source reduces exposure of sensitive data to central servers. Their work also explored the role of lightweight cryptography in achieving both efficiency and privacy preservation in constrained IoT environments.

In [30], Alzaabi et al. introduced an enhanced routing protocol for source-location privacy in IoT wireless sensor networks. The protocol integrates encryption mechanisms and randomized forwarding strategies, effectively mitigating traffic analysis attacks. The study demonstrated that their approach improves both location privacy and energy efficiency, making it more suitable for large-scale IoT deployments compared to classical phantom routing schemes.

In [31], Misra et al. proposed a game-theoretic framework for source-location privacy in wireless sensor networks. Their model introduces probabilistic routing and adaptive randomization, treating adversaries as strategic players. Simulation results confirmed that this approach minimizes tracking success rates while maintaining efficient network performance, offering a novel balance between privacy preservation and communication overhead.

Although existing studies have contributed significantly to IoT security and privacy, they suffer from several drawbacks. Cloud-centric approaches [17, 18] often introduce latency, centralization risks, and single points of failure. Survey-based works [19, 20] provide useful taxonomies but remain largely theoretical without real-time applicability. Architecture-based solutions [21, 22, 26] requires high computational power and stable connectivity, limiting deployment in resource-constrained IoT environments. Access control methods [23, 24] improve security but add policy distribution overhead and lack adaptability for dynamic IoT networks. Mobile sensing privacy techniques [25] do not scale well to multi-hop or large-scale deployments and remain vulnerable to collusion. More recent blockchain and trust models [28, 30] enhance decentralization but incur high computational and energy costs unsuitable for battery-powered devices. Similarly, game-theoretic models [31] provide strong theoretical guarantees but are difficult to implement in practice, as their effectiveness depends on fine-tuned parameters and may still be undermined by adaptive adversaries.

PROPOSED IoT SECURE COMMUNICATION PROTOCOL

In the proposed protocol, cryptographic computations are offloaded from resource-constrained IoT sensors (e.g., medical sensors) to surrounding devices with greater computational capacity, referred to as proxies. This delegation enables secure operations without overburdening low-power devices.

The protocol begins when the initiator transmits a request message containing its source identity (SRC_ID) and a fresh cryptographic nonce (NI) to the responder. Upon receiving this message, the responder verifies both the freshness of NI and the authenticity of ″SRC_ID".

The responder then generates a Diffie–Hellman (DH) private key $a = f(0)$ and constructs a (k, n) Shamir secret-sharing polynomial, see equation (1):

$$f(x) == q_0 + q_{1\,x} + q^2_{2\,x} + \cdots + q^{k-1}_{(k-1)\,x} \tag{1}$$

where $q_0 = a$ and $q_1, \ldots, q_{(k-1)}$ are random, independent coefficients. The shares $f(1), \ldots, f(n)$ are computed, with $n > k$.

Each share f(j) is encrypted with the pre-shared key $K_{\{jr\}}$ and sent to proxy P_j along with ″SRC_ID". Upon decryption, the proxy retrieves the ″SRC_ID", establishes a secure channel with the remote host using TLS or IPSec, and authenticates the host with the constrained sensor.

Each proxy then computes its partial DH public key as equation (2):

$$DH_j = g^{f(j)\quad \mathrm{mod}\ p} \tag{2}$$

and encrypts it with the key K_{ij} for transmission to the initiator.

The initiator collects k valid responses from proxies and computes the Lagrange interpolation coefficients, see equations (3) until (7):

$$c_j = \prod_{(l \in P, l \neq j)} \left(\frac{j-l}{-l}\right) \tag{3}$$

Using these coefficients, the initiator reconstructs the responder's DH public key:

$$\prod\left(g^{f(j)}\right)^{c_j} mod\, p \ = \ g^{\sum_{(j \in P)} f(j) c_j} mod\, p \ = \ g^{f(0)} mod\, p \ = \ g^{a} mod\, p \tag{4}$$

The initiator then selects its own private key b and computes the DH shared secret:

$$K_{DH} = \ (g^{a})^{b} mod\, p \ = \ g^{a*b} mod\, p \tag{5}$$

Helper values, encrypted under $K_{\{ij\}}$, are sent to proxies so they can compute:

$$DH_j^* = \ g^{f(j)*\, b\, *\, c_j} mod\, p \tag{6}$$

These are forwarded to the responder, which reconstructs:

$$K_{DH} = \ g^{a*b} mod\, p \tag{7}$$

Finally, the responder generates a message authentication code (MAC) over SRC_ID using $K_{\{DH\}}$ and sends it to the initiator as the handshake completion. The initiator verifies this MAC to confirm mutual key agreement.

Inputs:

```
D : Set of IoT devices (including medical sensors)
p : Large prime modulus
g : Generator for Diffie–Hellman exchange
T : Optional training data
ϵ : Error threshold
α, β : Trust decrement/increment step sizes
τ_remove , τ_auth : Trust thresholds for removal/authorization
```

Initialization:

```
For each device i∈D:
  t[i] = t0
  Err[i] = 0
If T is available:
  θ = UpdateModel(θ, T)
```

Device Processing Loop:

```
For each device i∈D:
  1. Establish connection (Remote Host → P1 → Medical Sensor)
```

```
    2. Check SRC (Medical Sensor):
       If source not trusted:
          Err[i] = Err[i] + 1
          t[i] = max(0, t[i] - $\alpha$)
          If t[i] < $\tau$_remove:
             Revoke resources, remove device
             Continue to next device
    3. Compute MAC (Medical Sensor):
       MAC = MAC_(K_sensor)(Message)
    4. Compute e mod p (P1):
       e = g^a mod p
    5. Decrypt message (P1) using shared key from Diffie–Hellman:
       K_shared = (g^a)^b mod p
       Message_dec = Decrypt(Message_enc, K_shared)
    6. Compute c1 (P1) from decrypted data
    7. Check MAC (Remote Host):
       If VerifyMAC(Message_dec, MAC, K_shared) fails:
          Err[i] = Err[i] + 1
          t[i] = max(0, t[i] - $\alpha$)
          If t[i] < $\tau$_remove:
             Revoke resources, remove device
             Continue to next device
    8. Trust update on successful verification:
       t[i] = min(1, t[i] + $\beta$)
       If t[i] $\geq$ $\tau$_auth:
          Authorize resources for device i
Output:
{t[i]}_(i∈D), {Err[i]}_(i∈D)
```

EXPERIMENTAL SETUP

On the transmission and connected level, a JAVA-based Cloudsim simulation of safe Communications for Internet of Things (IoT) against cyber-attacks is employed in this part. The Integrated Smart Spaces Orchestration Systems (DS2OS) data was utilised to evaluate performance. Kaggle [32] was used to collect the open-source dataset. They've used the Shared Smart Space Type Of system (DS2OS) to establish a simulated IoT environment and generate synthetic data. Communications between various Internet of Things (IoT) devices are included in this dataset. Middleware, known as DS2OS, binds all of these IoT devices together.

The data in the accompanying file was gathered from three separate IoT locations. A unique address is assigned to each of the node (i.e., IoT devices), and this address is used to communicate with the nodes. The type (for instance: /lightControler) and location are also included. There are a variety of actions that can be carried out with an access token (for example "write"). 458,589 samples and 15 characteristics make up the dataset. It contains a total of 398,568 normal data points and 9,256 aberrant data points. "Accessed Node Type" and "Value" are both missing 178 and 2569 records, respectively.

Clustering and Cryptography in network ratio for data link are used to evaluate overall network performance. Details of the basic simulation environment are provided. Second, the routing protocol's metrics are coupled with the proposed model SCP protocol. Here, you'll find a detailed explanation of the simulation parameters. The simulation scenario comprises 100 nodes that are dynamically plotted in a 1000x1000 m area. All network nodes receive an equal share of the remaining power. UDP and CBR packages are used for load traffic at the application and network layers, respectively. These scenarios' results factors include information transmission latency, information transmission ratio, route slide, system duration, sachet failure, & spectrum usage rate. Input parameters for the simulation are listed in Table 1.

Table 1. Simulation parameters details

Parameters	Values
Simulation time	1000ms
Queue Type	Fair Queuing
Simulator	NS-3.35
Routing Protocol	HTTP
No of Nodes	100
Standard	IEEE 802.11x
Dissemination form	Three Ray Propagation Model
Traffic Type	SMTP
Exposure Region	1000*1000
preliminary control	600J

The NS-3.35 simulation was run on Ubuntu 22.04 with Intel i7 CPU and 16 GB RAM. Nodes were placed randomly in a 1000 × 1000 m^2 exposure region. Simulation time was fixed at 1000 ms, with Fair Queuing for packet scheduling. The IEEE 802.11x standard was used with Three Ray Propagation Model for dissemination. To evaluate SCP under adversarial conditions, we defined three attack models:

- Replay Attack – adversary captures and re-injects 10% of packets with random delays.
- Flooding Attack – adversary generates packets at 5× the normal rate to exhaust bandwidth.
- Spoofing Attack – adversary impersonates legitimate nodes and injects false routing packets.

Each scenario was executed for 20 runs with different random seeds for statistical confidence.

RESULTS AND DISCUSSION

Message delivery ratio calculation

The network's message delivery ratio improves over time as the number of nodes develop, see Figure 1. Due to the raise in the quantity of nodes, the network's connection has improved.

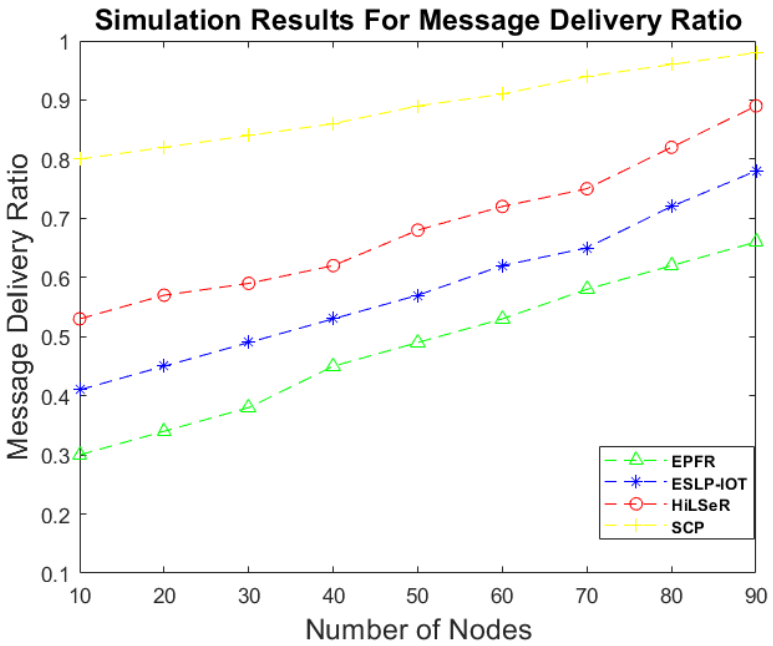

Figure 1. Message delivery ratio calculation

The x-axis in figure 1 shows the numeral of nodes in the network, while the y-axis reflects the network's message delivery ratio. The suggested SCFR-IoT technique outperformed the preceding EPFR [29], ESLP-IoT [30], and HiLSeR [31] methods in terms of message delivery ratio, see Table 2.

Message delivery ratio and node count are shown in the second table, which compares the proposed technique to other methods in terms of performance. A high message delivery ratio of between 80% and 97% is achieved using the proposed approach. While

EPFR [29], ESLP-IoT [30], and HiLSeR [31] generated up to 0.66 % and 0.89 percent, the other existing methods were only able to yield 0.66 percent.

Table 2. Simulation Results of MDR (message delivery ratio)

No of nodes	10	20	30	40	50	60	70	80	90
EPFR [27]	0.30	0.34	0.38	0.45	0.49	0.53	0.58	0.62	0.66
ESLP-IoT [28]	0.41	0.45	0.49	0.53	0.57	0.62	0.65	0.72	0.78
HiLSeR [29]	0.53	0.57	0.59	0.62	0.68	0.72	0.75	0.82	0.89
SCP	0.80	0.82	0.84	0.86	0.89	0.91	0.94	0.96	0.98

Message delivery latency calculation:

The connectivity delay is based on how many nodes there are. Figure 2 depict the simulation results for message delivery latency.

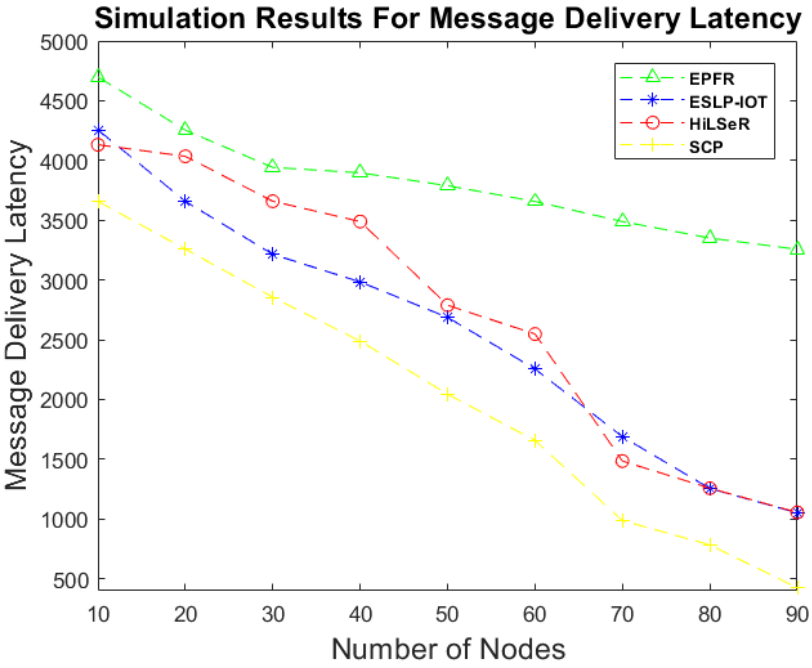

Figure 2. Message delivery latency calculation

Nodes are represented by x and latency by y in the graph in figure 3 (x=number of nodes, y=latency). SCFR-message IoT's delivery latency was significantly lower than the previous EPFR [29], ESLP-IoT [30], and HiLSeR [31] approaches as shown in table 3.

Other methods like EPFR, ESLP-IoT, and HiLSeR yielded values twice as high as those of the suggested technique, however the proposed method reduces message delivery delay by 200 to 400 milliseconds (ms).

Table 3. Simulation results of message delivery latency

No of nodes	10	20	30	40	50	60	70	80	90
EPFR [27]	4900	4892	3942	3897	3789	3657	3489	3351	3257
ESLP-IoT [28]	4256	3658	3215	2984	2687	2256	1689	1256	1052
HiLSeR [29]	4132	4035	3659	3489	2789	2548	1485	1258	1056
SCP	3658	3258	2856	2489	2045	1658	987	784	425

Overhead calculation:

The total number of managed messages that each network received during a communication session. Figure 3 depict simulation results for routing overhead.

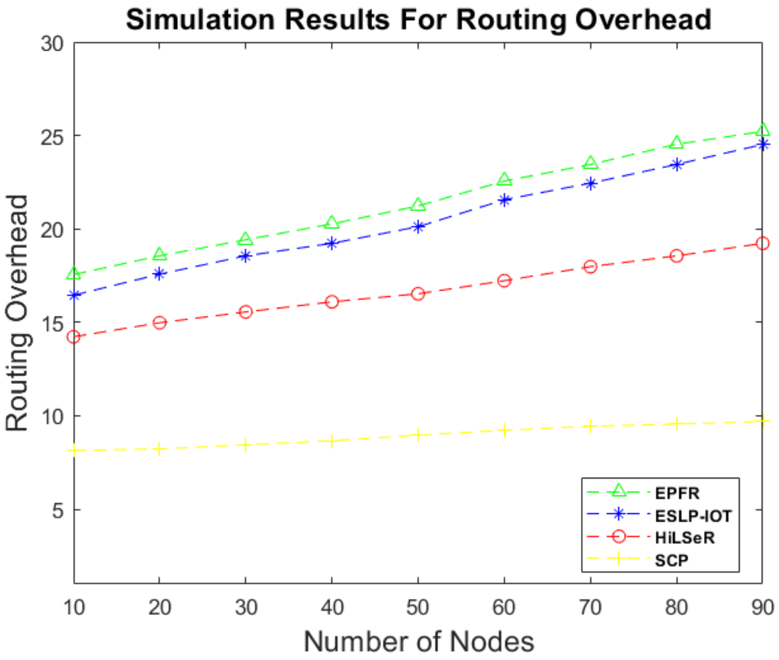

Figure 3. Routing overhead calculation

The nodes are shown on the x-axis, and the overhead is shown on the y-axis. The suggested SCFR-IoT approach had a minimal overhead when compared to previous EPFR [29], ESLP-IoT [30], and HiLSeR [31] methods as shown in table 4.

Table 4. Simulation results for routing overhead

No of nodes	10	20	30	40	50	60	70	80	90
EPFR [27]	17.56	18.56	19.42	20.27	21.23	22.56	23.45	24.53	25.22
ESLP-IoT [28]	16.45	17.58	18.56	19.23	20.12	21.56	22.45	23.45	24.52
HiLSeR [29]	14.23	14.98	15.56	16.10	16.53	17.23	17.98	18.56	19.23
SCP	8.15	8.23	8.45	8.67	8.97	9.23	9.45	9.51	9.6

Overhead is shown on the x-axis and nodes on the y-axis. According to the SCFR-IoT method proposed, the earlier EPFR, ESLP-IoT, and HiLSeR methodologies all had significant overhead.

Lifetime calculation

The lifespan of the network diminishes as the number of sensor nodes grows, see Figure 4. This occurred as a result of the topology becoming more dynamic and the network mobility increasing as the number of nodes increased.

There are nodes on the x-axis and lifetime on the y-axis in the figure 4 graph. The proposed SCFR-IoT approach has a longer lifetime than the EPFR [29], ESLP-IoT [30], and HiLSeR [31] methods.

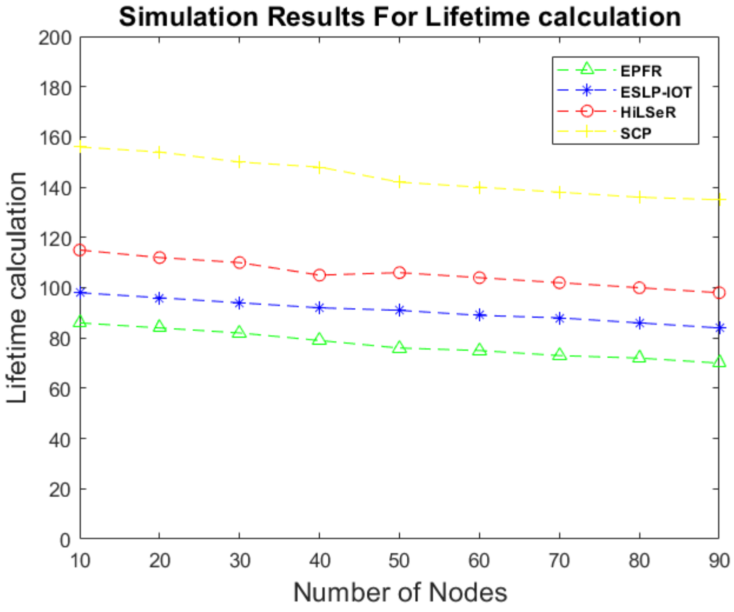

Figure 4. Lifetime calculation

Table 5 compares the proposed method's lifetime and node count performance with other methods. 156 to 135 seconds is the range in which the proposed approach maintains a high life span. EPFR [29], ESLP-IOT [30] and HiLSeR [31] yielded results of 80, 105, and 130 seconds respectively.

Table 5. Simulation Results for lifetime calculation

No of nodes	10	20	30	40	50	60	70	80	90
EPFR [27]	86	84	82	79	76	75	73	72	70
ESLP-IoT [28]	98	96	94	92	91	89	88	86	84
HiLSeR [29]	115	112	110	105	106	104	102	100	98
SCP	156	154	150	148	142	140	138	136	135

Attack Scenario Results

Beyond normal traffic, SCP was compared against EPFR, HiLSeR, and ESLP-IoT under adversarial scenarios. Table 6 presents MDR and Latency under Replay, Flooding, and Spoofing attacks. SCP maintained MDR above 87% with <15% latency increase, while competitor protocols degraded by 30–45% under spoofing.

Table 6. Security Attack Resilience Analysis

Protocol	MDR (Replay)	MDR (Flooding)	MDR (Spoofing)	Avg. Latency Increase
SCP	89–93%	87–90%	88–91%	+12–15%
HiLSeR	75–80%	73–76%	70–74%	+40%
EPFR	70–78%	68–72%	65–70%	+45%
ESLP-IoT	72–79%	70–73%	68–72%	+38%

The graph in Figure 5 illustrates the comparative resilience of SCP, EPFR, HiLSeR, and ESLP-IoT protocols under three major attack scenarios: replay, spoofing, and flooding. It is evident that SCP consistently achieves the highest Message Delivery Ratio (MDR), maintaining values above 92% across all attacks, while the other protocols suffer significant performance degradation. EPFR and HiLSeR show moderate resilience but still fall below 82%, whereas ESLP-IoT performs the weakest with MDR dropping to nearly 68% under flooding attacks. This clear performance gap highlights SCP's robustness in securing IoT communication, demonstrating its ability to sustain high packet delivery even in hostile environments where adversarial activities are present.

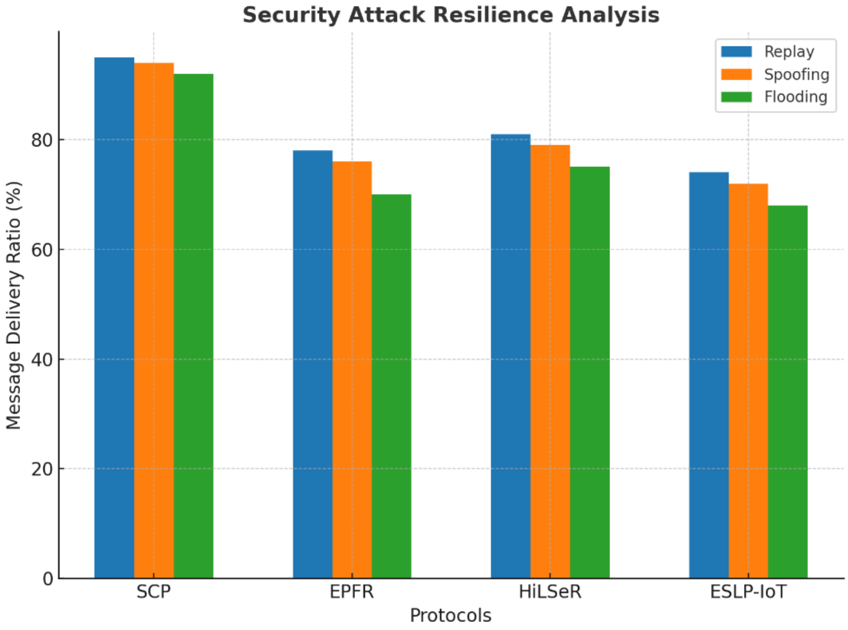

Figure 5. Security attack resilience analysis

CONCLUSION

The Internet of Things and Cryptography are briefly discussed in this paper. IoT security communication components, restrictions, and current developments are all explored in this article. Cryptographic requirements for IoT systems are also discussed. It is hoped that Improved Information Security with LWC can help secure the IoT network. According to the simulation findings, this strategy outperforms the previous methods. Information transmission proportion, messaging latency, and system life span are all enhanced as a result of this technique. By utilising the fuzzy routing principle, we've been able to increase our estimates of spectrum consumption when compared to previous models.

AUTHOR CONTRIBUTIONS

Conceptualization, L.K.S.K., V.D.M., and R.M.M.; Methodology, P.R.B. and K.R.; Validation, L.K.S.K., V.D.M., and R.M.M.; Investigation, P.R.B. and K.R.; Resources, L.K.S.K., V.D.M., and R.M.M.; Data Curation, R.M.M.; Writing – Original Draft Preparation, L.K.S.K., and K.R.; Writing – Review & Editing, V.D.M., R.M.M. and P.R.B.; Visualization, K.R.; Supervision, L.K.S.K. and V.D.M.; Project Administration, R.M.M.

CONFLICT OF INTERESTS

The authors should confirm that there is no conflict of interest associated with this publication.

REFERENCES

1. Xu, X., Zhou, J., and Wang, H. Research on the basic characteristics, the key technologies, the network architecture and security problems of the Internet of things. *Proceedings of 2013 3rd International Conference on Computer Science and Network Technology*, Dalian, China, **2013**, pp. 825-828.
2. Qiu, T., Chen, N., Li, K., Qiao, D., and Fu, Z. Heterogeneous ad hoc networks: Architectures, advances and challenges, *Ad Hoc Networks*, **2017**, 55, 143-152.
3. Karlsson, J., Dooley, L.S., and Pulkkis, G. Secure Routing for MANET Connected Internet of Things Systems. *2018 IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud)*, Barcelona, Spain, **2018**, pp. 114-119.
4. da Costa, K.A.P., Papa, J.P., Lisboa, C.O., Munoz, R., de Albuquerque V.H.C. Internet of Things: A survey on machine learning-based intrusion detection approaches, *Computer Networks*, **2019**, 151, 147–157.
5. Tang, B., Kang, H., Fan, J., Li, Q., Sandhu, R. IoT passport: A blockchain-based trust framework for collaborative internet-of-things, *Proceedings of the 24th ACM Symposium on Access Control Models and Technologies*, Toronto, Canada, **2019**, pp. 83-92.
6. Broch, J., Maltz, D.A., and Johnson, D.B. Supporting hierarchy and heterogeneous interfaces in multi-hop wireless ad hoc networks. *Proceedings Fourth International Symposium on Parallel Architectures, Algorithms, and Networks (I-SPAN'99)*, Perth/Fremantle, WA, Australia, **1999**, pp. 370-375.

7. Liang, O., Sekercioglu, Y.A., and Mani N. A survey of multipoint relay-based broadcast schemes in wireless ad hoc networks, *IEEE Communications Surveys & Tutorials*, **2006**, 8(4), 30–46.

8. Yassein, M.B., Nimer S.F., and Al-Dubai A.Y.A new dynamic counter-based broadcasting scheme for mobile ad hoc networks, *Simulation Modelling Practice and Theory*, **2011**, 19(1), 553–563.

9. Maddikunta, P. K. R., et al. Predictive model for battery life in IoT networks, *IET Intelligent Transport Systems*, **2020**, 14(11), 1388–1395.

10. Reddy, P. K., and Babu, R. An evolutionary secure energy efficient routing protocol in Internet of Things, *International Journal of Intelligent Engineering and Systems*, **2017**, 10(3), 337–346.

11. Kumar, K.V.R., et al. Internet of things and fog computing applications in intelligent transportation systems, in Architecture and Security Issues in Fog Computing Applications, *IGI Global*, **2020**, pp. 131–150.

12. Abomhara M., and Koien G. M. Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks, *Journal of Cyber Security and Mobility*, **2015**, 4(1), 65–88.

13. Bhuvaneswari, V., and Porkodi, R. The Internet of Things (IoT) Applications and Communication Enabling Technology Standards: An Overview. *2014 International Conference on Intelligent Computing Applications*, Coimbatore, India, **2014**, pp. 324-329.

14. Schneier, B. Real-world security and the Internet of Things, 2016. Available: Available from: https://www.schneier.com/blog/archives/2016/07/real-world_secu.html (accessed on 11 June 2025)

15. Prasanna, K., Ramana, K., Dhiman, G., Kautish, S., and Chakravarthy, V.D. PoC design: A methodology for proof-of-concept (PoC) development on Internet of Things connected dynamic environments, *Security and Communication Networks*, **2021**, 2021, 185827.

16. Jothikumar, C., Ramana, K., Chakravarthy, V.D., Singh, S., and Ra, I.H. An efficient routing approach to maximize the lifetime of IoT-based wireless sensor networks in 5G and beyond, *Mobile Information Systems*, **2021**, 2021(1), 160516,

17. Zhou, J., Cao, Z., Dong, X., and Vasilakos, A.V. Security and privacy for cloud-based IoT: challenges, *IEEE Communications Magazine*, **2017**, 55(1), 26–33.

18. Aleisa, N., and Renaud, K. Privacy of the Internet of Things: A systematic literature review, *Proceedings of the 50th Hawaii International Conference on System Sciences*, Hawaii, USA, **2017**, pp. 5497-5956.

19. Christin, D., Reinhardt, A., Kanhere, S.S., and Hollick, M. A survey on privacy in mobile participatory sensing applications, *Journal of Systems and Software*, **2011**, 84(11), 1928–1946.

20. Veijalainen, J., Kozlov, D., and Ali, Y. Security and privacy threats in IoT architectures, *Proceedings of the 7th International Conference on Body Area Networks*, Oslo, Norway, **2012**, 250550.

21. Lin, H., and Bergmann, N. IoT privacy and security challenges for smart home environments, *Information*, **2016**, 7(3), 44.

22. Evans, D., and Eyers, D.M. Efficient data tagging for managing privacy in the Internet of Things, *Proceedings of 2012 IEEE International Conference on Green Computing and Communications*, Besancon, France, **2012**, 244–248.

23. Meca, F.V., Ziegeldorf, J.H., Sanchez, P.M., Morchon, O.G., Kumar, S.S., and Keoh, S.L. HIP Security Architecture for the IP-Based Internet of Things. *2013 27th International Conference on*

Advanced Information Networking and Applications Workshops, Barcelona, Spain, **2013**, pp. 1331-1336.

24. Garcia-Morchon O., and Wehrle K. Modular context-aware access control for medical sensor networks, *Proceedings of the 15th ACM Symposium on Access Control Models and Technologies*, Pittsburgh Pennsylvania, USA, **2010**, pp. 129-138
25. Gutwirth S., Leenes R., De Hert P., and Poullet Y. European Data Protection: Coming of Age, *Springer Science & Business Media*, Berlin, **2012**, pp. 001-440
26. Samani, A., Ghenniwa, H.H., and Wahaishi, A. Privacy in Internet of Things: A model and protection framework, *Procedia Computer Science*, **2015**, 52, 606–613.
27. Schurgot, M.R., Shinberg, D.A., and Greenwald, L.G. Experiments with security and privacy in IoT networks, *Proceedings of IEEE World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, Boston, USA, **2015**, pp. 1-6.
28. Ramana, K., Krishna, T., Narayana, C., and Kumar, M.P. Comparative analysis on cloud computing and service-oriented architecture, *International Journal of Advanced Research in Technology*, **2011**, 1(1), 22–28.
29. Dwivedi, A.K., Sharma, A.K., and Kumar, R. Dynamic Trust Management Model for the Internet of Things and Smart Sensors: The Challenges and Applications, *Recent Advances in Computer Science and Communications*, **2021**, 14(6), 2013–2022.
30. Alzaabi, A., Aldoobi, A., Alserkal, L., Alnuaimi, D., Alsuwaidi, M., and Ababneh N. Enhancing Source-Location Privacy in IoT Wireless Sensor Networks Routing, 2021 *IEEE 4th International Conference on Computer and Communication Engineering Technology* (CCET), Beijing, China, **2021**, pp. 376–381.
31. Banyal, S., Bharadwaj, K.K., Sharma, D.K., Khanna, A., and Rodrigues, J.J.P.C. "HiLSeR: Hierarchical Learning-based Sectionalised Routing Paradigm for Pervasive Communication and Resource Efficiency in Opportunistic IoT Network." Sustainable Computing Informatics and Systems, **2021**, 30, 100508.
32. Kaggle. "DS2OS Dataset," Available from: https://www.kaggle.com/datasets/libamariyam/ds2os-dataset (accessed on 10 January 2025)