# 3S-IoT an Algorithm to make the Network Secured and Smart

**Maneesh Pant** (✉ maneeshgbpuat@gmail.com)
ABES Engineering College, Ghaziabad
**Sachin Kumar** (✉ sachinagnihotri16@gmail.com)
South Ural State University, Chelyabinsk, Russia https://orcid.org/0000-0003-3949-0302
**Rahul Kumar Sharma** (✉ rahulpccs1988@gmail.com)
KIET Group of Institutions, Ghaziabad, India
**Ahmed Alkhayyat** (✉ ahmedalkhayyat85@iunajaf.edu.iq)
The Islamic University, Najaf, Iraq

**Research Article**

**Keywords:** IoT Devices; Smart devices; GKE; DDoS; MiTM

**DOI:** https://doi.org/10.21203/rs.3.rs-92971/v2

# 3S-IoT: An Algorithmic Approach to Smart and Secure IoT Network

Maneesh Pant[1], Sachin Kumar[2,*], Rahul Kumar Sharma[3], Ahmed Alkhayyat[4]

[1]Computer Science Department, ABES Engineering College, Ghaziabad, Uttar Pradesh, India; maneeshgbpuat@gmail.com

[2,*]Big Data and Machine Learning Lab, South Ural State University, Chelyabinsk, Russia; sachinagnihotri16@gmail.com

[3]Computer Science & Engineering, KIET Group of Institutions, Ghaziabad, Uttar Pradesh, India; rahulpccs1988@gmail.com

[4]College of Technical Engineering, The Islamic University, Najaf, Iraq; ahmedalkhayyat85@iunajaf.edu.iq

**Abstract:** The growing and the widespread existence of the Internet of Things (IoT) has made our lives easier and more convenient. However, it still needs to dominate challenges, such as efficiency, security, and high energy consumption, to enrich innovative IoT-based applications. Unicast communication is used for small-scale applications. Multicast is preferable in large-scale communication because it allows efficient transmission with fewer resources and is utilized in various IoT applications. Multicast traffic involves actuator control to handle critical applications. Securing multicast traffic is complex as it needs an efficient and flexible Group Key Establishment (GKE) protocol. Therefore, this paper presents a temper proof of a three-level security model that can maintain the efficiency and security of IoT and multicast communications. The first authentication is done at network linking, where a 256-bit keyless encryption technique has been employed. Machine learning-based chaotic map key generation authenticates the GKE as the second-level authentication. Finally, Message Digest Algorithm 5 (MD5) establishes the system key. 3S-IoT is smart to detect any tempering with the devices. It stores the signature footprints of the connected devices. The algorithm is equipped to report any attempt to change or temper a device. 3S-IoT can thwart attacks such as Distributed Denial of Service (DDoS), Man-in-the-Middle (MiTM), and phishing. The numerical analysis is done by evaluating energy consumed, bandwidth, and the time taken to check the robustness of the proposed model. The results show that 3S-IoT can efficiently deal with the attacks. The work's authenticity is validated by comparing the proposed work with existing benchmark algorithms.

**Keywords:** IoT Devices; Smart devices; GKE; DDoS; MiTM

## 1. Introduction

*IoT* is the technology that hackers look at with greedy eyes. Internet means a network open to vulnerability, such as Distributed Denial of Service (DDoS). Connecting IoT devices in homes is simple these days; for example, the lights of a house use IoT switches like ‘sonoff’ and control them through a mobile phone. ‘Sonoff’ devices use a five-byte value for their ID to establish a connection. The first two bytes specify the device type, and the remaining three represent a random number. These switches use the same specific ID pattern for the multiple devices they support, which makes them vulnerable to brute-force attacks. By 2025, around 75 billion devices will be connected to IoT [1-4], which means that more people could be exposed to attacks without security.

Malware is one of the favorite tools of hackers. Hacking IoT using malware put forwarded in 2016. The hackers used Mirai IoT Botnet malware to find devices that were still using the factory default username and password [5]. Medical devices use IoT devices to a great extent. Cardiac devices from St. Jude were hacked [6]. They hacked the devices by accessing their transmitter. Using the same approach, hackers hacked Owlet Wi-Fi baby [7], the heart-monitoring smart device. The work presented in [8] shows that CCTV surveillance devices have gullible points. The study shows that over 100,000 wireless Internet Protocol (IP) cameras provide less protection. TRENDnet webcam transmits the user’s login and password over the internet in simple text [9]. Even their mobile application similarly kept the consumer details.

The cars we drive these days are very fragile to attacks. By using CAN, bus hackers hacked Jeep SUV [10,11]. The firmware update weakness was exploited. The hackers may hijack the vehicle over the Sprint cellular network and may control the speed. A lethargy to change the factory-set username password helped the hackers to attack. An estimated

100 Million home gadgets are highly receptive to attack [12]. Figure 1 shows different services which can be considered for IoT. The figure sums up different networks (Smart home, Cellular and healthcare network) and the places where hackers exploit to carry out the attacks such as MiTM, DDoS.

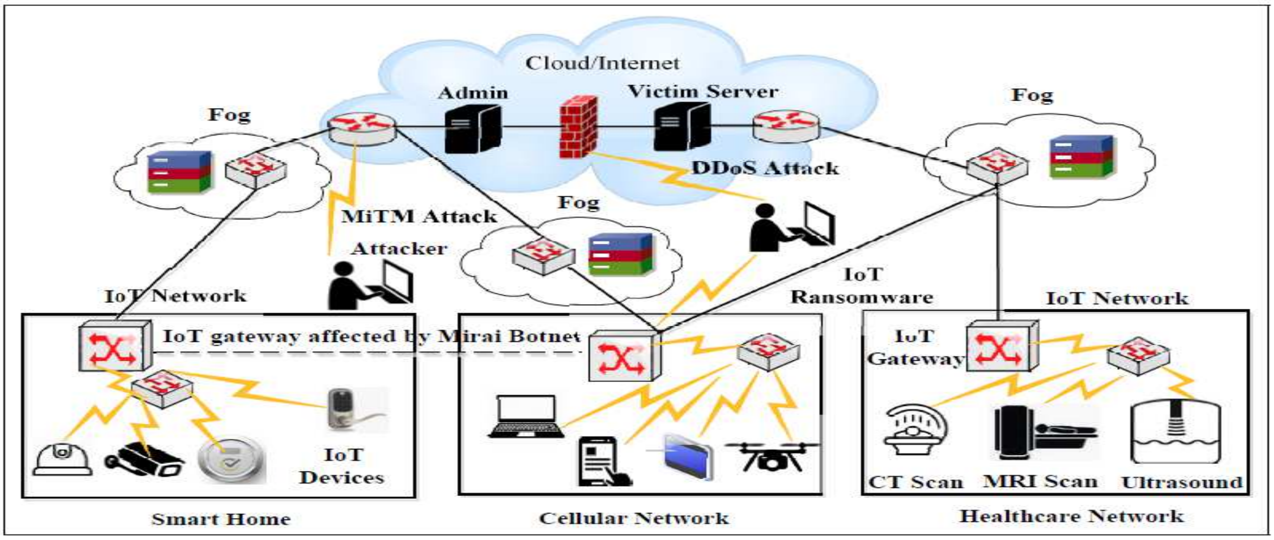
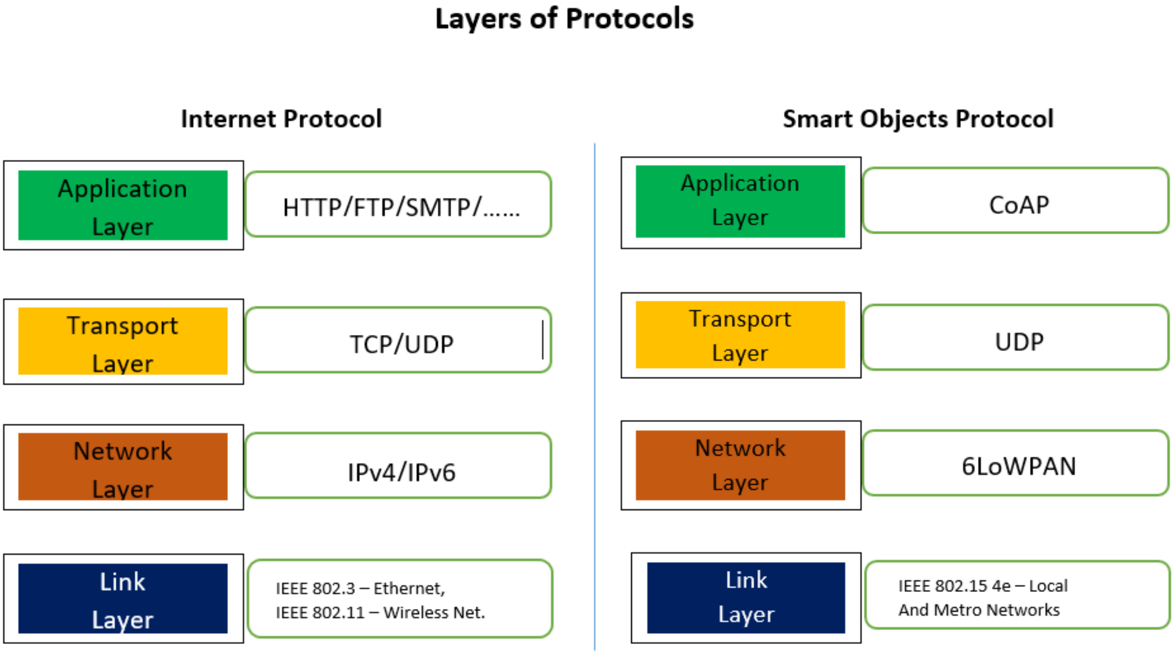


**Figure 1.** Shows the different IoT networks [16]

Figure 2 shows comparison of protocols used on the Internet and Smart devices. In 'Smart Objects Protocol', the network layer shows a Low Power Wireless Personal Area Networks (6LoWPAN) protocol.



Layers of Protocols

| Internet Protocol | | Smart Objects Protocol | |
|---|---|---|---|
| Application Layer | HTTP/FTP/SMTP/…… | Application Layer | CoAP |
| Transport Layer | TCP/UDP | Transport Layer | UDP |
| Network Layer | IPv4/IPv6 | Network Layer | 6LoWPAN |
| Link Layer | IEEE 802.3 – Ethernet,<br>IEEE 802.11 – Wireless Net. | Link Layer | IEEE 802.15 4e – Local<br>And Metro Networks |

**Figure 2.** Comparison of Internet Protocols and Smart object protocols [17]

The principle of IPv6 over 6LoWPAN derives from the belief that "the Internet Protocol can and should be extended to even the smallest devices. Also, low-power machines with minimal computing resources should be able to engage in the

IoT. IoT devices have specific functions and little room for robust security mechanism as the aim is to reduce the footprints. The transmission is heterogeneous which makes it difficult to adopt a standard protection method. The end-users are not aware of the vulnerability of these devices and do not even change their default username and password. In most of the encrypted transmissions, a key is passed to be deciphered at the receiver's end [13-15]. If one breaks the key one can hack the network easily.

## 2. Related Work

The Li et al., focused on the protection of privacy in Smart Grid buildings [18]. The work presumes that the key server and the trust centre are always available, but there is no discussion about security. Navneet presented Smart Meter's Secure Key Distribution Protocol which mainly concentrated on preventing man-in-the-middle attack [19]. The paper presents only a security review with no assessment of the results. Luca proposed Vehicle-to-vehicle communications in ad hoc networks [20]. As new members join, they themselves specify their predetermined leave period according to which batch leave operations are done. The paper assumes that every member is aware of the exact time to leave the party, which is not always be preferred.

Beside specific applications, different authentication schemes have also been proposed by various researchers, for instance, Jang in proposed a scheme "Marker Hash-Tree". It proposed device authentication without involving the central authority [21]. Sharaf proposed a fingerprinting authentication protocol for IoT devices. It has a transfer learning method which could mitigate the emulation attack effectively [22]. Sciancalepore proposed a key management scheme along with device authentication [23]. The proposed model could handle *fast re-keying*, *replay attack*, and *robust key negotiation.* Li proposed heterogeneous signcryption scheme. Their design is based on the model Identity-based Access Control (IBAC). Furthermore, their scheme makes use of bilinear pairing operations. Owing to the use of IBC and bilinear matching operations their scheme is expensive in terms of overhead computation [24]. Braeken proposed an efficient and distributed authentication protocol for smart homes. The model has a low computation cost, but the communication cost is high [25]. Luo suggested an IoT cross-domain efficient access control protocol for WSNs. The model enables an Internet user to connect with a smart computer in a CLC environment with specific network parameters [26]. Owing to the use of CLC and bilinear matching operations their scheme is therefore expensive in terms of overhead computation.

Xu suggests a two-factor mutual authentication and a key agreement scheme to minimize the computational costs based on elliptic curve cryptography (ECC), that would allow the use of dynamic identity to provide anonymity [29]. Yan suggested a device verification system based on biometrics [30]. But the scheme is vulnerable to the *replay attack*, and *word guessing attack*. Mishra proposed an enhanced scheme for biometric authentication using random numbers. His schemes have issues of efficiency when best quantum algorithm is selected for solving Shortest Vector Problem (SVP) and Closest Vector Problem (CVP) [31]. Also, issue of storage arises due to huge matrix operations. Tan expanded the security specifications of two-factor authentication schemes to three-factor authentication systems, that are mutual identification, password and biometric anonymous repositories, and three-factor encryption systems [32]. Guo initially suggested a messy map-based password authentication scheme for the e-healthcare information network, which avoids linear exponential computation or scalar elliptic curve multiplication found in conventional authentication schemes [33]. The scheme does not maintain user privacy and double-secret keys inefficiency. Lee in [34] proposed an improved scheme that could solve Guo's vulnerability. Lee [34] and Jiang [35] improvised [33] scheme. Moon [37] noticed that both Lee's [34] and

Jiang’s [35] systems are vulnerable to the assault on service misuse and proposed a stable authentication scheme to fix the security vulnerability. Moon [36] explained that the stable authentication scheme [34] & [35] is not safe from *replay attack, impersonation attack, an intruder attack*. They suggest a changed authentication system to correct such security vulnerabilities. Roy claimed that the currently associated scheme suffered from server attack denial and did not have a revocation function. Roy suggested a remote authentication with three lightweight factors which can withstand different information attacks [37]. Lu found out that there are still some vulnerabilities in Chun's enhanced system, such as a vulnerability to the user impersonation attack, it lacked local authentication and a violation of session key protection. Lu introduced a three-factor authentication scheme [38].

Most of the research work carried out is tied to a certain type of application such as smart grids, internet of vehicles, etc, none of it is generic. Besides, those researches work on just one or two aspects of IoT assuming that the conditions of the application scenario are static, which is not the case always. IoT application scenarios are dynamic and have a varying nature regarding the network access technology, type of application, state of members and key servers and the load on them. The research till now have either focused mostly on rekeying protocol or very specific to an application [39-44]. Duan introduced light weight key management system (KMS) [45]. KMS updates the keys which can easily hackers can easily break, the research is more theoretical. Therefore, in this work, the authors to introduce a 3S-IoT model. The model adapts to the dynamic nature of IoT scenarios and provides temper proof 3-level security. Each level of security can also be used independently for securing any communication and encrypting the images.

The main contribution of this study is as follows:

We have designed a three-level security for IoT devices.

- The first authentication is at network linking where we used to a 256-bite keyless encryption technique.
- At second level, we designed a Machine learning-based chaotic map group key generation authentication, moreover, we designed MD5 based encryption to stablish connection with the device.
- Our proposed model can detect any tempering with the devices. It stores signatures of the connected devices. The algorithm reports any attempt to change or temper a device. The model takes only 76 KB space, including the image. This makes it ideal to use with low power consumption devices. The model can establish the connection very fast and the packet loss is very less. The proposed model can secure any type of network. The GK algorithm can securely transmit image over any network.

## 3. Methodology

This section of the paper briefly describes the Experimental Setup and the protocol considered followed by Objective Function and its explanation. Then steps to establish connection with sender and receiver are discussed. The paper aims at providing a three-tier safety to IoT. The main objective function mathematical represents the objectives of 3S-IoT.

### Setup

A smart IoT home network is setup using CCTV cameras, smart ACs, and Lights. The three groups are integrated over the cloud and connected to a Wi-Fi router with an ISP. To access the network over the cloud, Redmi Note 9 pro max is used. The required application is installed on the smartphone. The attacks are carried on using Kali Linux run on Ubuntu. Another Redmi note 7 is loaded with Wi-fi hacking applications to crack the wi-fi.

Power$\leftarrow$1 Mw

BW ← 256 kbps
Protocol ← 6LowPAN
Packets ← IPv6 (6LowPAN is used to send IPv6 packets over IEEE 802.15.4)
Network Protocol ← IEEE 802.15.4
Packet size ← 127 octets

### *3.1. Objective function*

There are three main objectives of the proposed model, establish a secured network connection, access group key and then access device securely. These objectives are mathematically represented by following Objective Function:

$$\left[\sum_{\forall I_0} L\left(B_{256}(I_0)\right) + \left[\sum_{n=1}^{100} predictor(T_{input}, T_{output}) \rightarrow \sum_{i=1}^{n} L_{Chaos}(f, P, t)\right] + \sum_{\forall I} MD_5(I)\right] \quad .......(1)$$

### *3.1.1 Explanation of Objective Function*

*1.* We took a 32X32 image and converted it into a 256-bit binary scalar matrix and then stored it on target network as it's ID. *Io* is the original image, Function $B_{256}$ converts it into 256-bit Encrypted image, and *L* convert the encrypted image into scalar. Working is explained in algorithms section. The algorithm uses the generated ID for network authentication.

*2.* Second, using linear regression generate a 9-digit ID. $T_{input}$ are the input values and $T_{output}$ are the output values. The input and output values are explained in the algorithm discussed in next sections.

*3.* Third, generate a sequence of 100 numbers using Lorenz map. We took 9-digit ID generated in above step as one of the input parameters. We use the generated key to authenticate the groups.

*4.* Finally, we took MD5 of the image to establish the connection with the device.

### *3.1.2 Steps to Establish Connection with Sender & Receiver*

Step1: Initiator and responder are created and assigned cloud ID

Step2: The initiator creates a multicast group MG = $G_1$, $G_2$….$G_{n-1}$ and generate separated $G_k$ IDs

Step3: An image is assigned to the initiator. Images are 32X32. Same is stored at the responder

Step4: The image is encrypted using 64-bit encryption, (first objective function). It is called $N_k$ (network key)

Step5: Once we encrypt the image, we have deleted the original image at the initiator

Step6: Convert the image to scalar

Step7: To establish connection initiator passes $N_k$ to the responder

Step8: Responder first reshapes the scalar matrix then, decrypts $N_k$ and matches with the stored image. A connection is established using (2)

$$Connection = \left\{\begin{matrix} 0 & if\ no\ match \\ 1 & if\ match\ found \end{matrix}\right\} \quad ..............(2)$$

Step9: Group key, $G_k$ is created using (3)

Step10: Using MD5 generates a Device Key $D_k$. Encrypted image is used for the purpose

Step11: Connection with the device is established if

$$Device\ Access = \begin{cases} 0 \ if\ no\ match \\ 1\ if\ G_{k\, match} \end{cases} and \begin{cases} 0 \ if\ no\ match \\ 1\ if\ D_{k\, match} \end{cases} \quad ..........(3)$$

## 4. Numerical Investigation

For the experimental purpose we designed a simulated programme using MATLAB. following sections explain the working in detail.

*4.1. Network key establishment using 128-bit image encryption*

We have proposed a unique authentication scheme based on images. Then, we have assigned each image to the network. Smart home, hospital and traffic system all the three networks are assigned a unique network key. For the experimental purpose, we take 32X32 greyscale images. 3S-IoT can work on any size of the image. We used small images, as IoTs do not have much storage space.

*Pseudocode 1: encryption at the initiator*

```
Setup
Collect greyscale images
Initialize required variables

Start
1. I ← read the greyscale image
2. [r, c] ← size(I)
3. I ← I/256 # convert to binary
4. $R_s$← fix random seed with device id
5. $b_n$ ←generate a set of [r x c] binary, random numbers
6. $I_e$ ← replace a least significant bit of I with $b_n$
7. $I_t$ ← reshape $I_e$ to (r x n) scalar matrix
```

The initiator requests the responder to establish the connection using the 128-bit encrypted image

*Pseudocode 2: Network key establishment with responder*

```
1. Get the image for the IP and MAC address stored at the server
2. Perform step 1 to 7 at the responder to get a 128-bit encrypted image
3. Applying eq(1) establish connection
```

*4.2. Group key establishment*

A group key is required if there are multiple IoT devices

*Pseudocode 3: GKE*

```
    Setup
    Initialize required variables
    Generate numbers using Machine Learning’s Linear Regression
    1: Fix Random seed
    2: For i = 1 to number of training counts:
                a, b, c, d ← generate random integers
        op ← a + (2*b) + (4*c) + (6*d)
        Input← {a, b, c, d}
        Output← op
3: predictor ← LinearRegression (number of jobs = -1)
4: output← predictor.fit (Input, Output)
5: Test_set ← Group ID
6: output ← predict Test_set using    (4 )

                                              $\sum_{n=1}^{100} predictor(T_{input,}T_{output})$            ………….(4)

                                              Here,
                                              n:number of counts
                                              predictor($T_{input}$, $T_{output}$): Predicted values, Linear Regression

Generate values using Lorenz Map
7. n← 100
8. L← generate Lorenz numbers using the equation in ( 5)

$\sum_{i=1}^{n} L_{chaos}\,(f, P, t)$                    …………….(5)

Here,
P: Predicted values
T: hundread random bumbers with a step of 0.01
f: $[\sigma \times (p1 - p2), t1 \times (rho - p3), p1 \times p2 - \beta \times p3]$
$\sigma$:10.0
rho:28.0
$\beta$:8.0/3.0

9. For several groups:
$G_{k(i)}$ ← assign to a group
```

```
End loop
10. Establish group access using    (3)
```

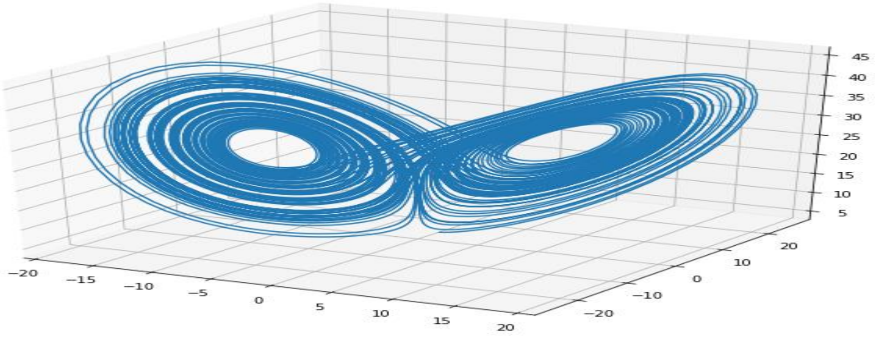


**Figure 3.** Lorenz map

The key generated after 4.2 is shown in Fig 3. The Lorenz map serves as the Group key.

### *4.3. Device Key generation and establishment*

Each device or an individual device, if a group of IoT is not there, is accessed using Pseudocode 4

*Pseudocode 4: Device Key establishment*

```
Setup
Initialize the required variables

1: For images in the folder do
I← read image(i)
Opt.method ← 'MD5'
V(i) ← DataHash (I, Opt) #DataHash is an inbuilt method
            End For
2: For i 1 to length of V do
          Device← V(i)
     End for
```

## 5. Authentication

3S-IoT is a keyless model. It is purely based on the algorithm designed. This section describes some of the attacks and how 3S-IoT mitigates them. The key security features are –

**a.** There is one to one access only. For example, we store CCTV's DVR's Mac address in the cloud server. When a user accesses a camera through mobile phone, we encrypt phone’s details like number, IP, MAC and authentication and store them on a cloud server. To establish a connection on another mobile, user will have to logout of the cloud server first.

**b.** OTP Authentication required for setup on a mobile

**c.** Factory set ID and passwords automatically reset during the first setup of devices. The user has to choose a username. A password generator pops up to generate a password, user cannot set the password of choice. Group key establishment as defined above is used to suggest a password to the user. After the first-time setup, there is no way a password can be changed unless the device is manually reset.

Once the user has the access to the device. Network key, Group Key, and Device keys are established.

## 6. Mitigation

The proposed scheme resets the authentication key every Δs seconds. Once the connection is established the reset is again initiated. For a new session, new authentication would be required. A delayed or replay attack won't work as the key would have changed by the time the user would try to break-in. To add to the complexity images have been used to establish a connection and that too in encrypted form. Moreover, the images are transmitted in a linear form.

A Trojan can break the code, but we took care of that also. Even when the entire system breaches, the attacker will still not be able to access the proposed program as the code produces a unique signature for the target computer when the application is installed on the network, and stores it in the code itself which is then recompiled into an executable file. Via Trojan, an attacker could be able to monitor the network but would not be able to access the machines because they would be searching for a local signature and even though the attacker could steal the code it would not work on his network because the new machine's signatures would not match. What the attacker would get will be just encrypted signal that could not be decrypted as the attacker will have neither the signature nor the algorithm to decode the message.

The Redmi Note 7 can crack a 6/9/12/16-character (alphanumeric) wi-fi password given by the user. But when the key generated by the proposed model is used as the password, the application returned a password which did not match with the original. Various attacks (given in table 1) using 'Kali' could not crack the keys and the passwords.

## 7. Experiments and Results

The work in the paper is simulated using MATLAB. The parameters considered for the robustness are - Energy consumed, bandwidth consumed, and time required. Equations 6 to 8 have been used for the calculations, to compare and analyse the proposed 3S-IoT algorithm.

**Table 1.** Comparison with previous related work. (Y): The technique used is secure against the security attribute.

| Security Attribute | [3] | Moon[36] | Roy[37] | Xu[39] | Liu[41] | Das[46] | 3S-IoT |
|---|---|---|---|---|---|---|---|
| **Stolen smart card or mobile device attack (SF1)** | | Y | Y | Y | Y | | Y |
| **Replay attack (SF2)** | Y | | Y | | Y | Y | Y |
| **Password guessing attack (SF3)** | Y | Y | Y | Y | Y | | Y |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Privileged insider attack (SF4)** | Y | Y | Y | Y | Y | | Y |
| **Known session key secrecy (SF5)** | Y | Y | Y | Y | Y | Y | Y |
| **Session key security (SF6)** | Y | Y | Y | Y | Y | Y | Y |
| **User impersonation attack (SF7)** | Y | Y | Y | Y | Y | Y | Y |
| **Server impersonation attack (SF8)** | Y | Y | Y | Y | Y | Y | Y |
| **Server-insider attack (SF9)** | | | | | Y | | Y |
| **Revocation of smart device (SF10)** | | | Y | | Y | Y | Y |
| **Secure mutual authentication (SF11)** | Y | Y | Y | Y | Y | | Y |
| **Password remote authenticate (SF12)** | | | | | Y | Y | Y |
| **Formal security analysis (SF13)** | | Y | Y | | Y | | Y |
| **Strong secure secret key (SF14)** | Y | | | | Y | Y | Y |
| **Group Key Establishment (SF15)** | | | | | | | Y |
| **Man, in the Middle Attack ((SF16)** | | | | | | Y | Y |
| **Phishing Attack (SF17)** | | | | | | | Y |
| **3-Tier Security (SF18)** | | | | | | | Y |
| **Malicious device deployment (SF19)** | | | | | | Y | Y |
| **ESL Attack (SF20)** | | | | | | Y | Y |

Table 1 shows a comparison of attacks the proposed model can mitigate. After comparison with [3], [36]- [37], [39], [41] & [46] we can observe that the existing algorithms have not taken into account some of the security features(SF) viz. SF15, SF17 and SF18. Whereas, 3S-IoT defends against these attacks.

**Table 2.** Functionality Comparison

| Parameter | Moon[36] | Roy[37] | Xu[39] | Liu[41] | Das[46] | Kaur[48] | 3S-IoT |
|---|---|---|---|---|---|---|---|
| **Attack Detection** | Y | | Y | Y | Y | Y | Y |
| **Automatic Remediation** | | | | | | Y | Y |
| **Applicability in IoT** | Y | Y | Y | Y | Y | Y | Y |
| **Scalability** | Y | Y | Y | Y | Y | Y | Y |
| **Dynamic System** | | | | | | Y | Y |
| **3-Level Security** | | | | | | | Y |
| **Large Number of Attacks** | | | | | | | Y |

Table 2 shows a comparison of functionality. The proposed model is flexible. It can be used for any type of IoT, small or big. We have compared Throughput and time delay with [46]. The proposed work focuses on energy consumed as well. It is going to play a decisive role when the network would grow. Higher energy consumption may result in network failure. The proposed work considers devices in a group. For the sake of testing, we divided the comparison into three groups having 5,11, and 17 devices in group 1,2, and 3 respectively [46].

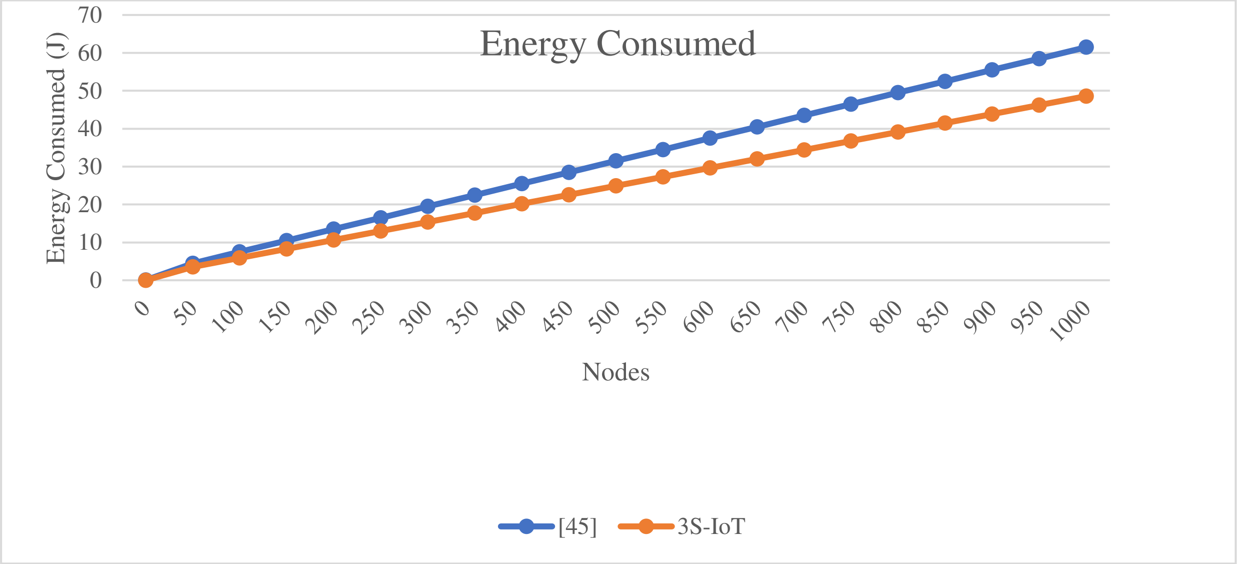


**Figure 4.** Energy consumed compared with [47]

As shown in Figure 4, the Energy consumed by 3S-IoT tends to remain constant with an increase in the number of devices. 3S-IoT saves 21% more energy than [47. It is likely that with an increase in the number of devices, the energy consumption increases. Low energy consumption is the default requirement of any network establishment. Higher the energy consumption lower would be the interest of the individuals to use them. Also, in devices may malfunction if their energy requirements are not met. We calculated the energy consumed by the proposed work using (6) .

$$E_c = \frac{\sum_{i=1}^{n}(E- e_i)}{n} \qquad ..........(6)$$

Here,

$E_c$: Energy Consumed

E: Total Energy

n: Number of Sensors

$e_{i:}$ Energy Required

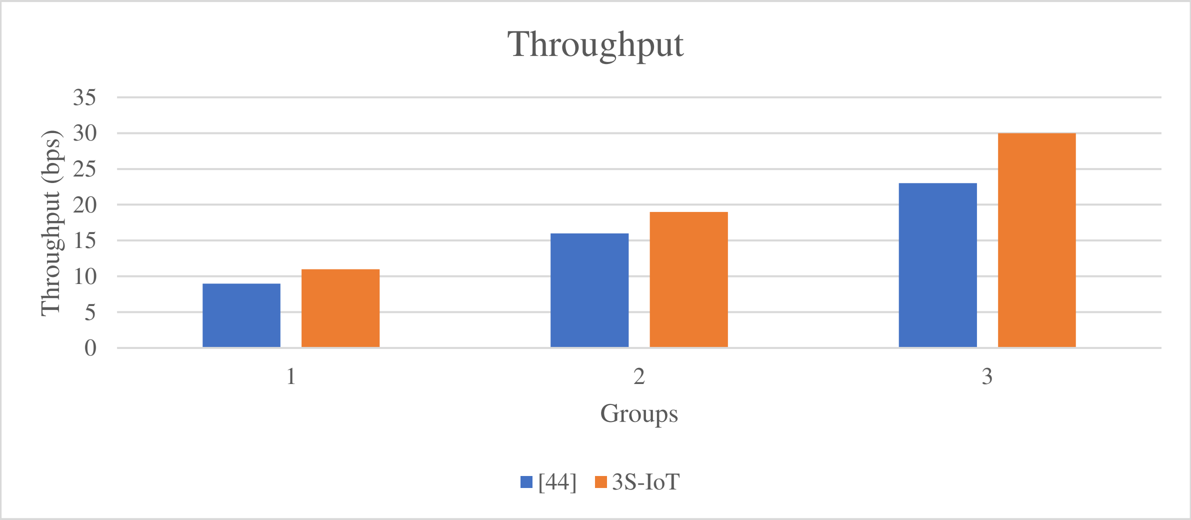


**Figure 5.** Throughput compared with [46]

In Figure 5, throughput another very important factor in estimating the cost of a model has been compared with [46]. IoT devices used at home or small offices should have a low Bandwidth requirement as there are limited resources available at such places. For example, if there are 10 IoT devices connected over a home network then the bandwidth available for the other devices would be very less. So, wither the IoT devices would have to compromise on the network availability or the other devices like Laptop, mobile phones etc. We calculated the bandwidth using (7) .

$$bw_c = \frac{\sum_{i=1}^{n}(Bw-bc_i)}{n} \qquad \text{................}(7)$$

Here,

$bw_c$ : Bandwidth consumed

Bw: Total Bandwidth

n: Number of Sensors

$bc_i$ : Bandwidth Required

The throughput (in bps) increases with an increase in the number of packets exchanged. This is a reflection of how many packets have been heard. 3S-IoT has a high throughput indicating that it has lesser packet loss when compared with [46]. Figure 6. compares 3s-IoT and [46] on time-delay parameter. The other important factor is the time taken in establishing the connection. Here, $T_{start}$ is the sending time of the packets and $T_{stop}$ is the receiving time of the packets. A complicated algorithm could take more time than the level of patience individuals has. We used equation (8) to calculate the time consumed.

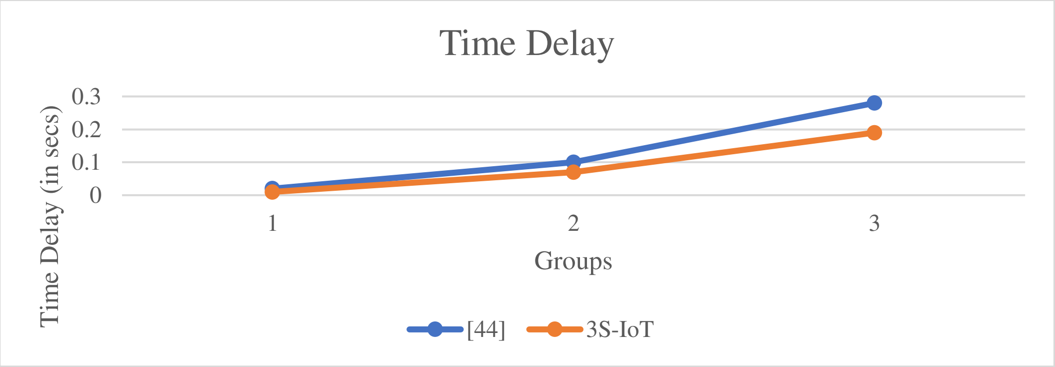


**Figure 6.** Time Delay compared with [46]

$$T_c = \sum_{i=1}^{n}(T_{stop} - T_{start}) \qquad \text{...........(8)}$$

Here,

$T_c$ : Time Consumed

$T_{start}$ : Start Time

$T_{stop}$ : Stop Time

N: Number of Sensors

As the devices increase in a group the delay increases as well. But, unlike [46] it is not a steep incline in case of 3s-IoT. Also, the delay is less.

## 8. Conclusion

Our secure IoT architecture provides privacy (through Black Networks), identity management and authentication (through Unified Registry), protected routing (through Trusted SDN) and protected key management framework. These four fundamental components of architectural security can be applied across any IoT framework. The model has three-level security. GK security is based on image encryption. Instead of images, random numbers can be used but hackers are smart to understand and crack it. The model takes only 76 KB space, including the image. This makes it ideal to use with low power consumption devices and standalone devices. The iterations are kept at minimum without compromising the complexity. A higher complexity is achieved with lower time and space consumption resulting in a fast connection and transmission. The proposed model can secure any type of network. The GK algorithm used in the model can securely transmit images over any network. Due to its design and low space requirement the model performs relatively well on the three parameters: time, energy, and bandwidth. The simulated attacks prove that the proposed work protects the network from known or unknown attacks of all kinds. Since hackers invent almost every day, there is 99% protection against Phishing or Malware. The proposed model protects against Trojan attacks as well. The system keeps a device signature so even if a hacker can install a Trojan, it will only be able to watch but won't be able to manage any device remotely. The attacker can see what is happening, for example, it can remotely watch the CCTVs but would not be able to control them. The model is not 100% protected against Trojan. The authors are working on it to make the protection 100%. Also, we are considering of making the sensors temper proof. The proposed work has hardware security of 80%. The authors are working on cognitive learning to achieve 100 per cent defence against all kinds of tampering and attacks.

**Funding:** No external funding was received.

**Data and Code availability:** Data and ode can be provided on request

**Acknowledgement:** We want to give thanks to the research facilities provided by ABES Engineering College, Ghaziabad in college premises. It greatly helped us to carry out our research work. Specially, the Do It Yourself (DIY) lab gave us a clear view of how IoT network works and thus helping us in getting better results.

**Conflict of interest/ Competing interests:** Authors have declared that there is no conflict for any author position and corresponding author.

**References**

1. Safai, B.; Monazzah, A. M. H.; Bafroei, M. B.; Ejlali, A.; Reliability side-effects in Internet of Things application layer protocols. In Proceedings of 2nd International Conference on System Reliability and Safety (ICSRS), Milan, Italy, 20/12/2017.
2. McKinsey Global Institute. Available online: https://www.mckinsey.com/~/media/McKinsey/Industries/Technology%20Media%20and%20Telecommunications/High%20Tech/Our%20Insights/The%20Internet%20of%20Things%20The%20value%20of%20digitizing%20the%20physical%20world/Unlocking_the_potential_of_the_Internet_of_Things_Executive_summary.pdf (accessed on 3/06/2019).
3. Statista Research Department. Available online: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/ (accessed on 12/07/2020).
4. United Nations, Department of Economic and Social Affairs, Population Division. Available online: https://population.un.org/wpp/Publications/Files/WPP2015_DataBooklet.pdf (accessed on 12/07/2020).
5. Kambourakis, G.; Kolias, C.; Stavrou, A. The Mirai botnet and the IoT Zombie Armies. In proceedings of *MILCOM IEEE Military Communications Conference (MILCOM), Baltimore, MD*, USA, 23/10/2017.
6. CNN Money. Available online: https://money.cnn.com/2017/01/09/technology/fda-st-jude-cardiac-hack (Accessed on 12/7/2020).
7. Information Security Buzz. Available online: https://www.informationsecuritybuzz.com/expert-comments/owlet-baby-wi-fi-monitor-worst-iot-security-2016/ (Retrieved on 15/07/2020).
8. Cusack, B.; Tian, Z. Evaluating IP surveillance camera vulnerabilities. In t*he Proceedings of 15th Australian Information Security Management Conference,* Edith Cowan University, Perth, Western Australia, *5/12/2017.*
9. The Register. Available on: https://www.theregister.co.uk/2013/09/05/ftc_slaps_trendnet_with_20_years_probation_over_webcam_spying_flaw/ (Accessed on 15/08/2020).
10. Forbes. Available on: https://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/?sh=6e1871b9228c (Accessed on 16/07/2020).
11. Security Zap. Available on: *https://securityzap.com/*files/Remote%20Car%20Hacking.pdf (Accessed on 16/07/2020)
12. Sivaraman, V.; Chan, D.; Earl, D.; Boreli, R. Smart phones attacking smart homes. In Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks (WiSec '16), Association for Computing Machinery, New York, USA, 18/07/2016.
13. Thomas, M.; Panchami, V. An encryption protocol for end-to-end secure transmission of SMS. Proceedings in International Conference on Circuits, Power and Computing Technologies [ICCPCT-2015], Nagercoil, India, 19/03/2015.
14. Zhou, X.; Tang, X.;. Research and implementation of RSA algorithm for encryption and decryption. In Proceedings of 6th International Forum on Strategic Technology, Harbin, Heilongjiang, 22/08/2011.

15. Bonde, S.; Bhadade, U. Analysis of Encryption Algorithms (RSA, SRNN and 2 Key Pair) for Information Security. In proceedings of International Conference on Computing, Communication, Control and Automation (ICCUBEA), Pune, India, 17/08/2017.

16. Chaudhary, R.; Aujla, G.S.; Kumar, N.; Zeadally, S. Lattice-Based Public Key Cryptosystem for Internet of Things Environment: Challenges and Solutions. *IEEE Internet of Things Journal 2019*, 6, 4897-4909.

17. Infinite Information Technology. Available on: http://www.infiniteinformationtechnology.com/iot-connectivity-iot-protocol-layers (Accessed on: 16/07/2020)

18. Li, D.; Zeyar, A.; Srinivas, S.; John, W.; Abel, S.;. Privacy Preservation Scheme for Multicast Communications in Smart Buildings of the Smart Grid. *Journal, Smart Grid and Renewable Energy (SGRE)* (2013), 04, 313–324.

19. Agrawal N. Secure Key Distribution Protocol with Smart Meter. In: *International Journal of Current Engineering and Technology* 2015, 5.

20. Veltri, L.; Cirani, S.; Busanelli, S.; Ferrari, G. A novel batch-based group key management protocol applied to the Internet of Things. *Elsevier Journal, Ad Hoc Networks 2013,* 11, 2724-2737.

21. Jang, S.; Lim, D.; Kang, J. An Efficient Device Authentication Protocol without Certification Authority for Internet of Things. *Wireless Personal Communication,* 2016*,* 91, 1681–1695.

22. Sharaf-Dabbagh, Y.; Saad, W. On the authentication of devices in the Internet of things. Proceedings in *IEEE 17th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM), Coimbra, Portugal, 2/06/2016.*

23. Sciancalepore, S.; Piro, G.; Boggia, G.; Bianchi, G. Public Key Authentication and Key Agreement in IoT Devices with Minimal Airtime Consumption. *IEEE Embedded Systems Letters,* 2017, 9, 1-4.

24. Li, F.; Han, Y.; Jin, C. Practical access control for sensor networks in the context of the Internet of Things. *Computer Communications* 2016, 89-90, 154-164.

25. Braeken, A.; Porambage, P.; Stojmenovic, M.; Lambrinos, L. eDAAAS: Efficient distributed anonymous authentication and access in smart homes. *International Journal of Distributed Sensor Network 2016*, 12,1-11.

26. Luo, M.; Luo, Y.; Wan, Y.; Wang, Z. Secure and efficient access control scheme for wireless sensor networks in the cross-domain context of the IoT. *Security and Communication Networks* 2018, 1-10.

27. Canetti; Krawczyk, H. Universally composable notions of key exchange and secure channels. Proceedings of International Conference on the Theory and Application of Cryptographic Techniques, Amsterdam, The Netherlands, 01/01/2002.

28. Abdalla, M.; Fouque, P.; Pointcheval, D. (2005). Password-based authenticated key exchange in the three-party setting. Proceedings in International workshop on Public Key Cryptography, *Springer, Berlin, Heidelberg, Public Key Cryptography*.

29. Xu, X.; Zhu, P.; Wen, Q.; Jin, Z.; Zhang, H.; He, L. A Secure and Efficient Authentication and Key Agreement Scheme Based on ECC for Telecare Medicine Information Systems. *Journal of Medical System* 2014, 38, 9994.

30. Yan, X.; Li, W.; Li, P.; Wang, J.; Hao, X.; Gong, P. A Secure Biometrics-based Authentication Scheme for Telecare Medicine Information Systems. *Journal of Medical Systems* 2013, 37, 1-6.

31. Mishra, D.; Mukhopadhyay, S.; Kumari, S.; Khan, M. K.; Chaturvedi, A. Security enhancement of a biometric based authentication scheme for telecare medicine information systems with nonce. *Journal of Medical System* 2014, 38(5), 41.

32. Tan, Z. A User Anonymity Preserving Three-Factor Authentication Scheme for Telecare Medicine Information Systems. Journal of Medical Systems, 2014, 38(3):16.

33. Guo, C.; Chang, C. C. Chaotic maps-based password authenticated key agreement using smart cards. *Communications in Nonlinear Science and Numerical Simulation* 2013*,* 18, 1433-1440.

34. Lee, T. An Efficient Chaotic Maps-Based Authentication and Key Agreement Scheme Using Smartcards for Telecare Medicine Information Systems. *Journal of Medical Systems* 2013*,* 37, 9986.

35. Jiang, Q.; Ma, J.; Lu, X.; Tian, Y. Robust Chaotic Map-based Authentication and Key Agreement Scheme with Strong Anonymity for Telecare Medicine Information Systems. *Journal of Medical Systems* 2014*,* 38.

36. Moon, J.; Choi, Y.; Kim, J.; Won, D. An Improvement of Robust and Efficient Biometrics Based Password Authentication Scheme for Telecare Medicine Information Systems Using Extended Chaotic Maps. *Journal of Medical Systems* 2016*,* 70.

37. Roy, S.; Chatterjee, S.; Das, A. K.; Chattopadhyay, S.; Kumari, S.; Jo, M. Chaotic Map-Based Anonymous User Authentication Scheme with User Biometrics and Fuzzy Extractor for Crowdsourcing Internet of Things. *IEEE Internet of Things Journal* 2018*,* 5, 2884-2895.

38. Lu, Y.; Li, L.; Pengand, H.; Yang, Y. A secure and efficient mutual authentication scheme for session initiation protocol. *Peer-to-Peer Networking and Application* 2016, 9,449-459.

39. Xu, X.; Zhu, P.; Wen, Q. A Secure and Efficient Authentication and Key Agreement Scheme Based on ECC for Telecare Medicine Information Systems. *Journal of Medical Systems* 2014, 38,9994.

40. Chain, K.; Chang, K. H.; Kuo, W. C.; Yang, J. F. Enhancement authentication protocol using zero-knowledge proofs and chaotic maps: ENHANCE-MENT AUTHENTICATION PROTOCOL. *International Journal of Communication System* 2014, 30.

41. Liu, W.; Wang, X.; Peng, W. Secure Remote Multi-Factor Authentication Scheme Based on Chaotic Map Zero-Knowledge Proof for Crowdsourcing Internet of Things. *IEEE Access* 2020, 8, 8754-8767.

42. Xie, Q.; Liu, W.; Wang, S.; Han, L. Improvement of a Uniqueness-and-Anonymity-Preserving User Authentication Scheme for Connected Health Care. *Journal of Medical Systems* 2014, 38.

43. Xu, L. D.; He, W.; Li, S. Internet of Things in Industries: A Survey. *IEEE Transactions on Industrial Informatics* 2014, 10, 2233-2243.

44. Lee, C.; Lin, T. H.; Chang, R., X. A secure dynamic ID based remote user authentication scheme for multi-server environment using smart cards. *Expert Systems with Applications* 2011*,* 38, 13863-13870.

45. Duan, L.; Li, Y.; Liao, L. Lightweight key management system for inter-node communication in IoT. *Proceedings of the 10th International Conference on the Internet of Things IoT '20. Association for Computing Machinery, New York, NY, USA,* Article 14, 1–8, October, 2020.

46. Das, A. K.; Wazid, M.; Yannam, A. R.; Rodrigues, J.; Park, Y. Provably Secure ECC-Based Device Access Control and Key Agreement Protocol for IoT Environment. *IEEE Access* 2019, 7, 55382-55397.

47. Gu, H.; Potkonjak, M. Efficient and secure group key management in IoT using multistage interconnected PUF. *Proceedings of the International Symposium on Low Power Electronics and Design* 2018*, 8*, 1-6.

48. Kaur, R.; Kaur, N.; Sood, S. K. Security in IoT network based on stochastic game net model. *International Journal of Network Mgmt.* 2017, 27.

# Figures

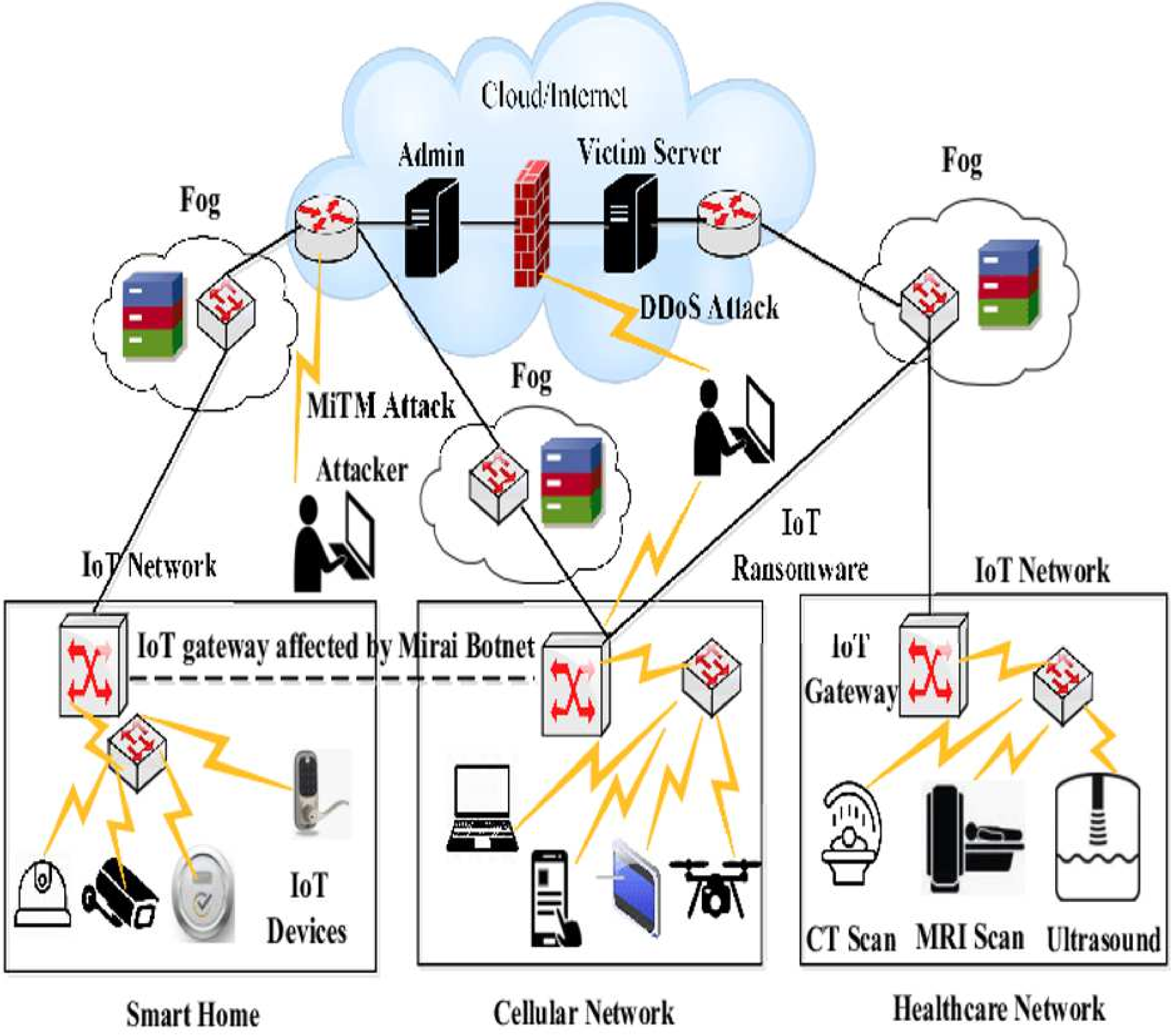
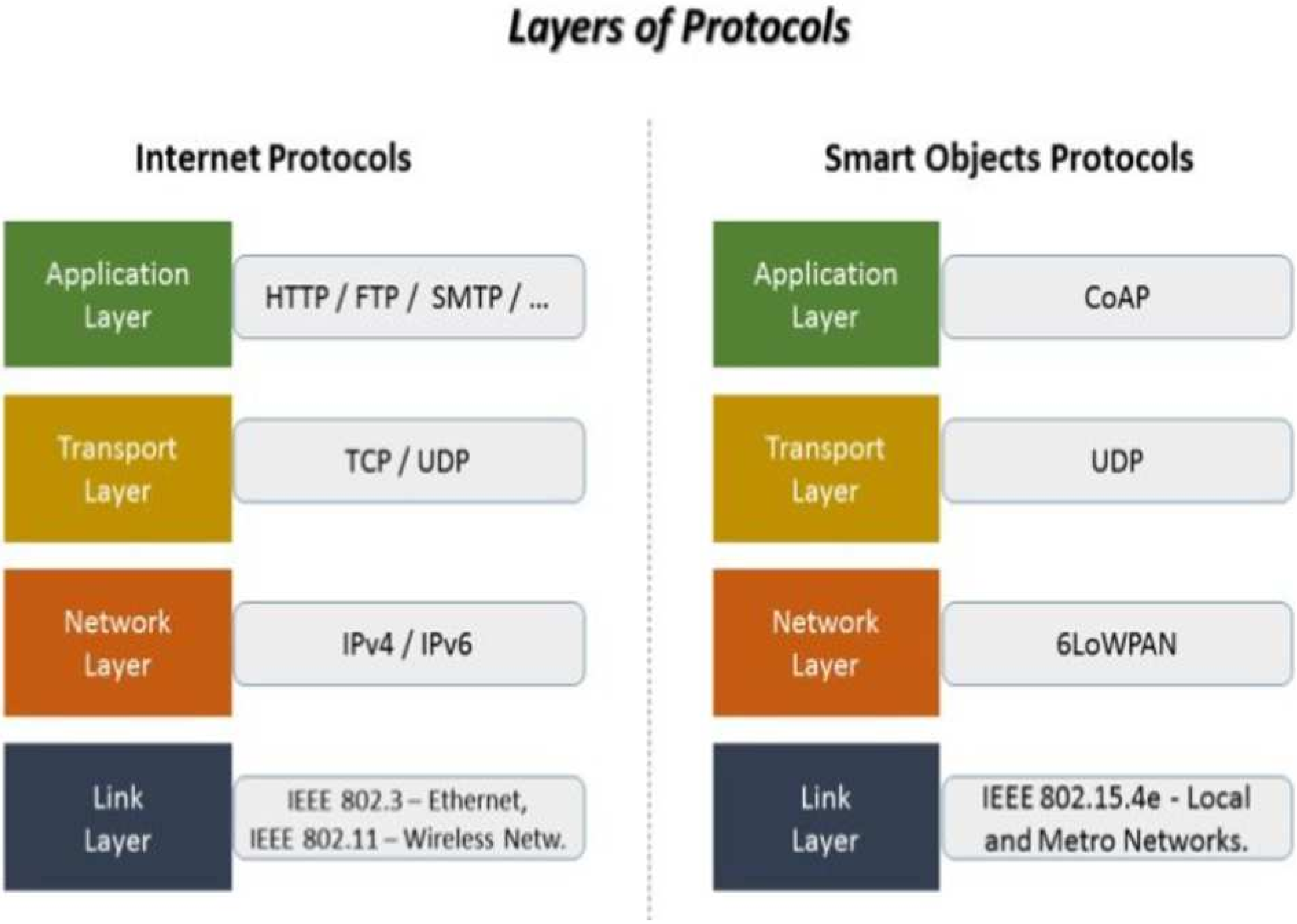


**Figure 1**

Shows the different IoT networks [16]



Layers of Protocols

| Internet Protocols | | Smart Objects Protocols | |
|---|---|---|---|
| Application Layer | HTTP / FTP / SMTP / ... | Application Layer | CoAP |
| Transport Layer | TCP / UDP | Transport Layer | UDP |
| Network Layer | IPv4 / IPv6 | Network Layer | 6LoWPAN |
| Link Layer | IEEE 802.3 – Ethernet,<br>IEEE 802.11 – Wireless Netw. | Link Layer | IEEE 802.15.4e - Local and Metro Networks. |

**Figure 2**

Comparison of Internet and Smart object protocol (http://www.infiniteinformationtechnology.com/iot-connectivity-iot-protocol-layers)

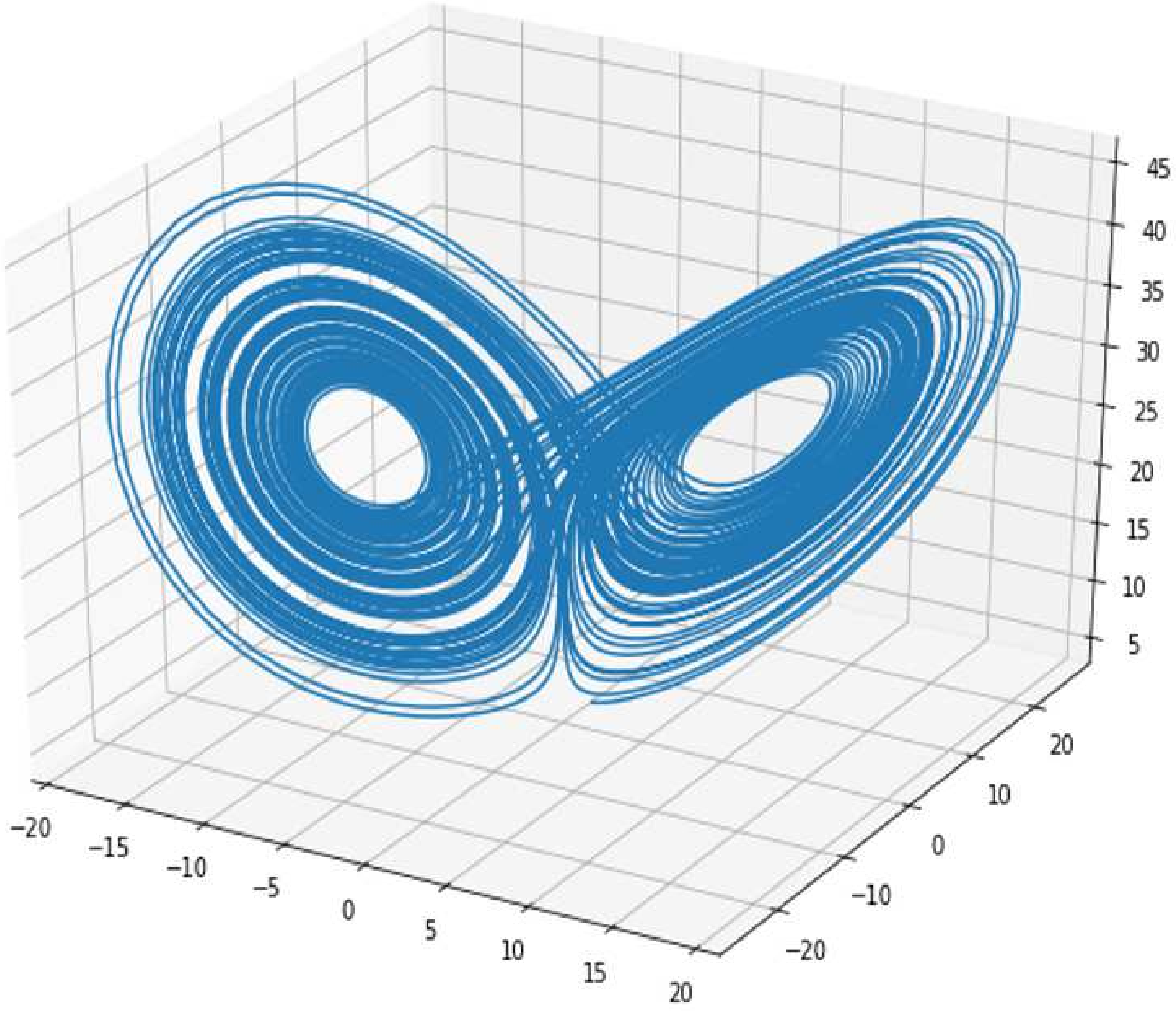


Figure 3

Lorenz map

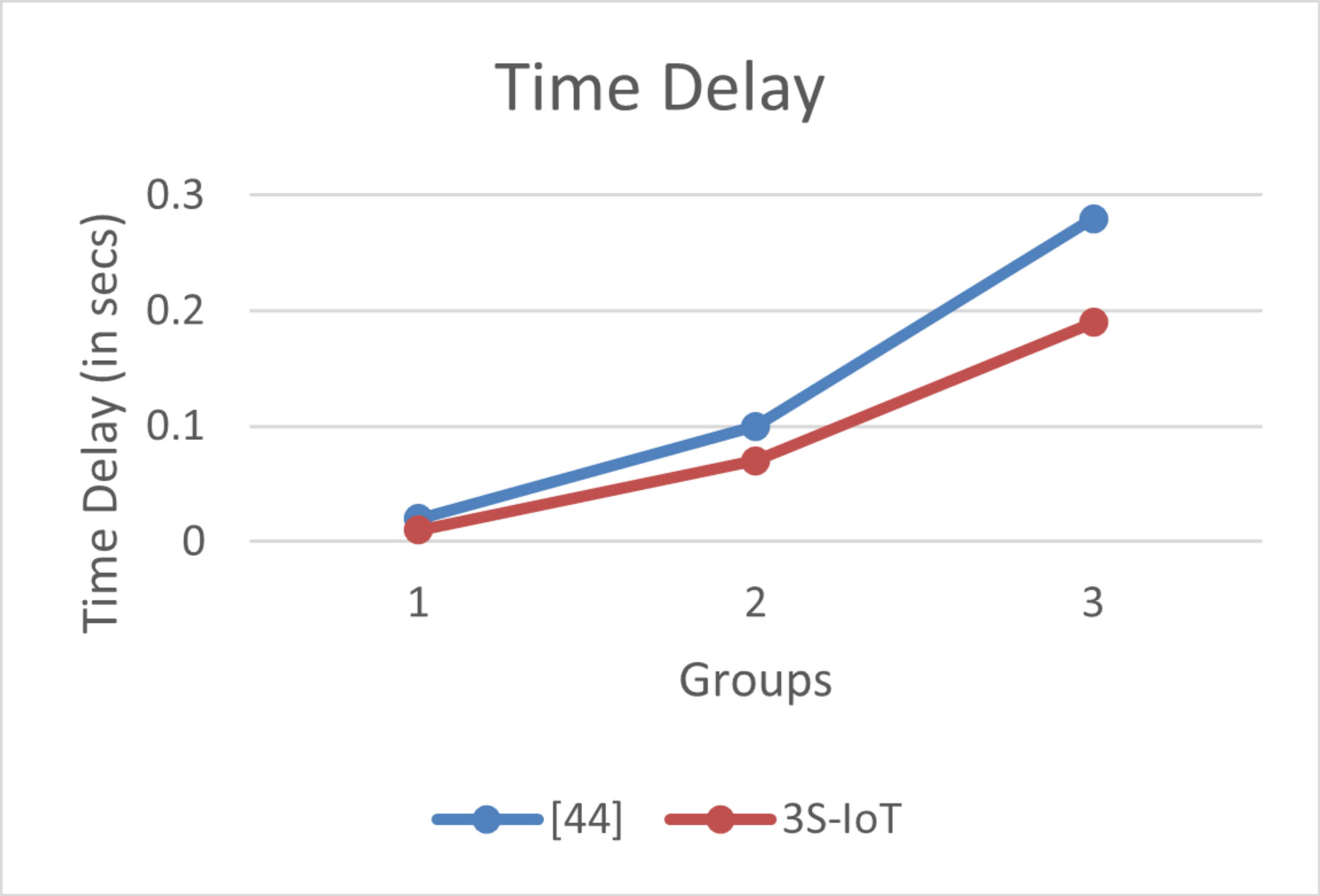


**Figure 4**

Time Delay

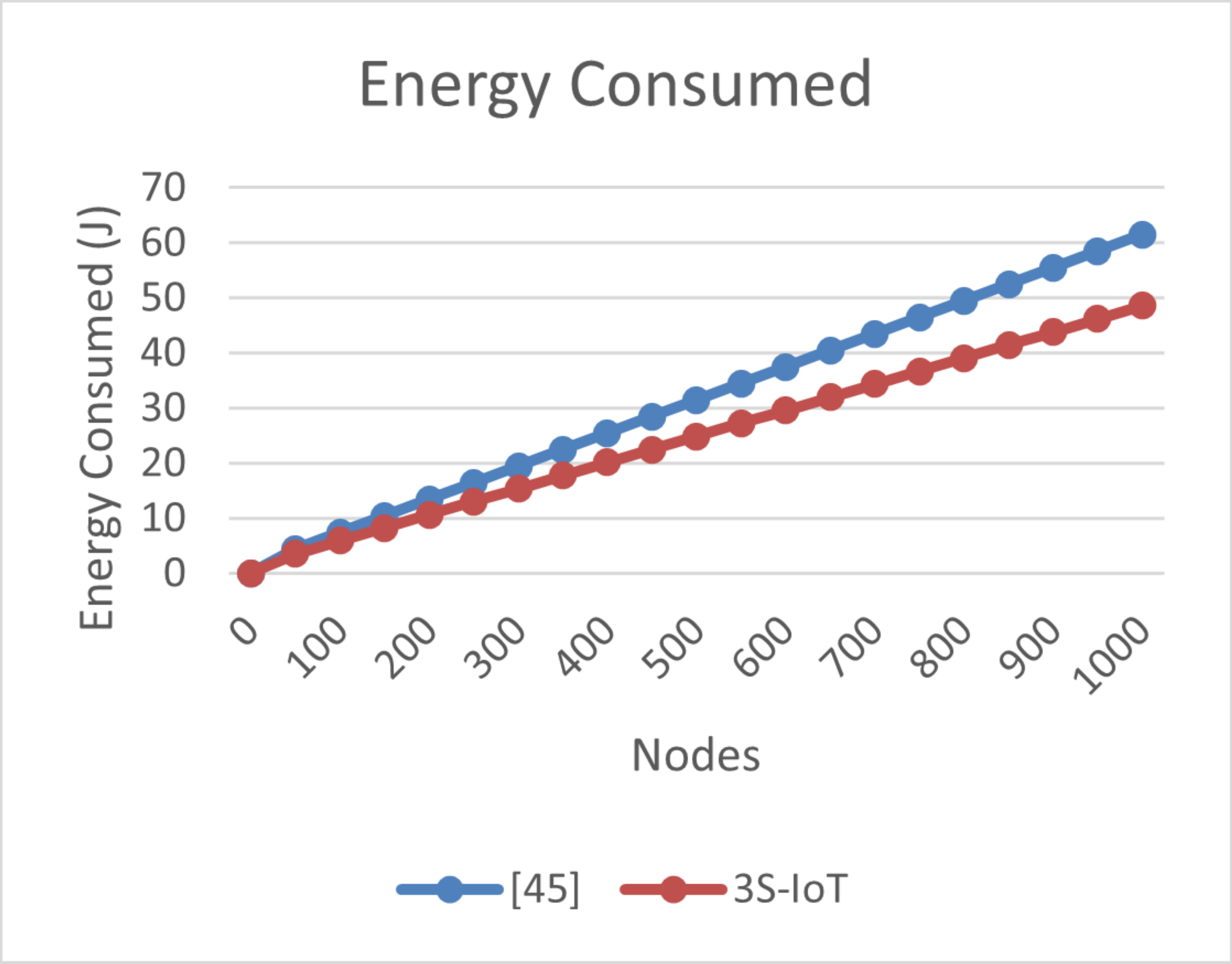


**Figure 5**

Energy consumed

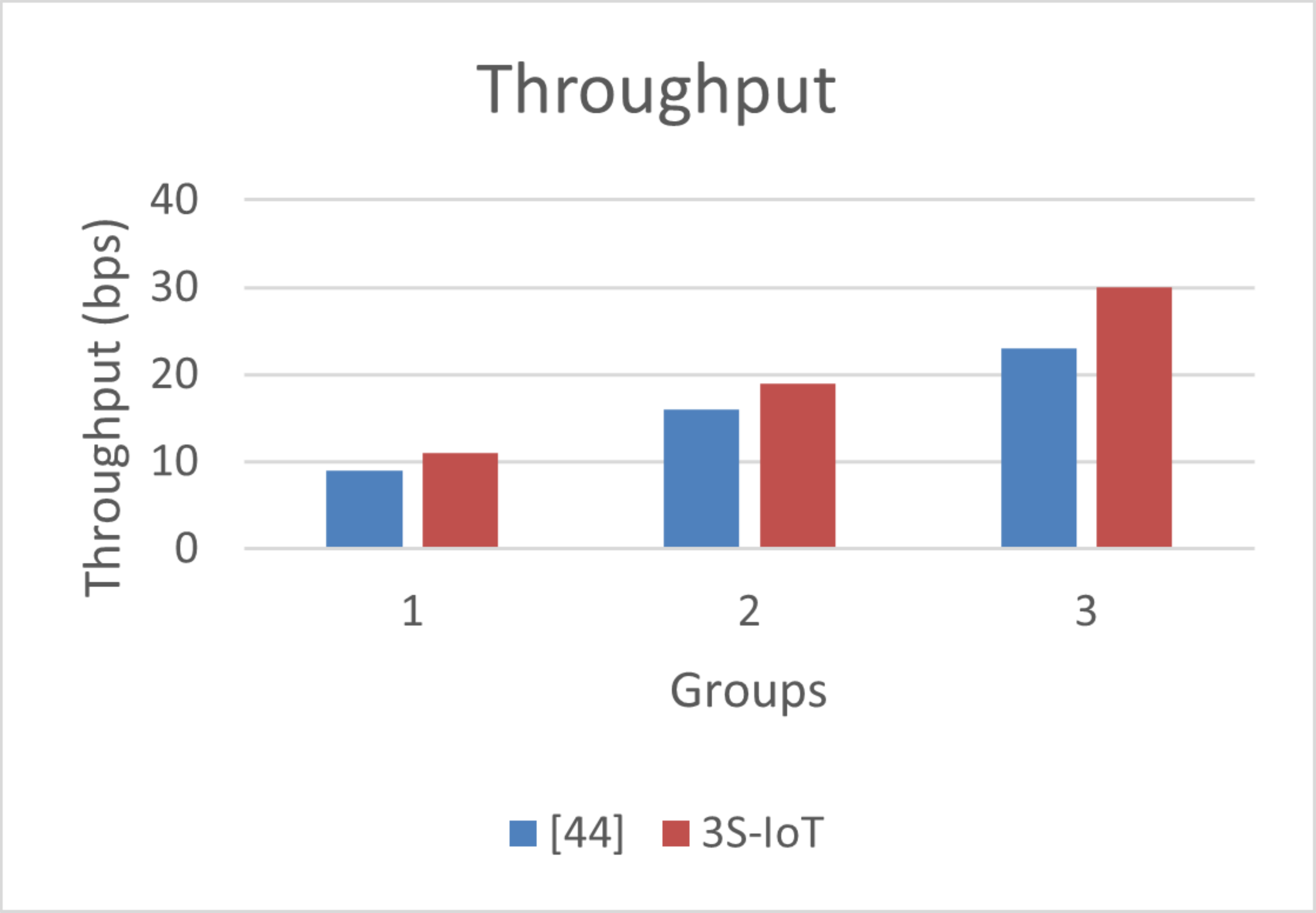


**Figure 6**

Throughput