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

maneesh pant (maneeshgbpuat@gmail.com)
College of Engineering Roorkee https://orcid.org/0000-0003-1029-2177
Brijmohan Singh
College of Engineering Roorkee
Dharam Vir Gupta
College of Engineering Roorkee

Research Article

Keywords: IoT devices, Smart devices, Secured IoT, Secured group key, Secured network key, Secured device key

Posted Date: March 29th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-236122/v1

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

Maneesh Pant [1*], Brijmohan Singh [2], Dharam Vir Gupta[3]

Abstract: The growing and widespread presence of Internet of Things (IoT) has made the lives of all comfortable and handy, but poses various challenges, like efficiency, security, and high energy drain, threatening smart IoT-based applications. Small applications rely on Unicast communication. In a group-oriented communication, multicast is better as transmission takes place using fewer resources. Therefore, many IoT applications rely on multicast transmission. To handle sensitive applications, the multicast traffic requires an actuator control. Securing multicast traffic by itself is cumbersome, as it expects an efficient and flexible Group Key Establishment (GKE) protocol. The paper proposes a three-tier model that can control the IoT and control multicast communications. The first authentication is at network linking where we used a 256-bit keyless encryption technique. Machine learning-based chaotic map key generation authenticates the GKE. Finally, MD5 establishes the system key. 3S-IoT is smart to detect any tempering with the devices. It stores signatures of the connected devices. The algorithm reports 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), phishing, and more. We calculated energy consumed, bandwidth, and the time taken to check the robustness of the proposed model. The results establish that 3S-IoT can efficiently deal with the attacks. The paper compares 3S-IoT with Benchmark algorithms.

Keywords IoT devices. Smart devices. Secured IoT. Secured group key. Secured network key. Secured device key

Declaration

Funding: NA
Conflict of interest/ Competing interests: NA
Availability of data and material: Data can be provided
Code availability: Code can be provided

Maneesh Pant
maneeshgbpuat@gmail.com

Brijmohan Singh
director@coer.ac.in

1,2 Department of Computer Science & Engineering, 7th K.M. on Roorkee (NH-58), Rehmadpur Vardhmanpuram, Haridwar Rd, Roorkee, Uttarakhand 247667, India

3 Department of Mathematics, 7th K.M. on Roorkee (NH-58), Rehmadpur Vardhmanpuram, Haridwar Rd, Roorkee, Uttarakhand 247667, India

1. Introduction

IoT is the technology which hackers look at with greedy eyes. Internet means a network of networks and a network could be open to vulnerability. DDoS is the most common of them. Connecting IoT devices in homes is simple these days. One can connect the devices, for example, ACs of a house using IoT switches like sonoff and control them through a mobile phone. An app configures an IoT switch, but the switch connects the device to the provider's cloud or a dedicated server. The server is on the internet that transmits the instructions to the device. One can understand how vulnerable it can be. It means that a user needs a secured server even for a smaller connection. Servers like AWS are secured but they are very costly. How can a switch like sonoff, available at 400 Rupees will be able to afford a server? Our CCTVs at home and offices are connected over the cloud too. Camera vendors either provide servers or, they outsource, which are not very secure. To check the vulnerability of the CCTVs a person can go to Google Dorks and easily find the open CCTVs. These CCTVs are easy to hack. Imagine IoT as a bug sitting in your home watching you all the time. 2025 would see about 75 billion devices connected to IoT [1-4].

Malware is one of the favourite tools of hackers. Hacking IoT using malware came up in 2016. To find devices that were still using the factory default username and password, the hackers used Mirai IoT Botnet malware [5]. These systems were hacked using this malware. Medical devices use IoT a lot. Cardiac devices from St. Jude were hacked [6]. They hacked the devices by accessing their transmitter. Using the same vulnerability, hackers hacked Owlet WiFi baby [7], the heart monitoring smart device. Research [8] show that CCTV surveillance devices have vulnerable points. The study [8] shows that over 100,000 wireless Internet Protocol (IP) cameras provide little to no protection. TRENDnet webcam [9] transmitted user's login and password over the internet in simple text. Even, their mobile application kept the consumer details the same way. The cars we drive these days are vulnerable to such attacks. Using CAN bus hackers hacked Jeep SUV [10,11]. The firmware update vulnerability was exploited. The hackers hijacked the vehicle over the Sprint cellular network. They could speed up the vehicle or even slow down. The consequences were disastrous. A habit to purchase a cheap and unsecured device, lethargy to change the factory-set username password helps the hackers to attack. 100 Million home gadgets are vulnerable to attack [12]. One can even hack the transmission if information is vulnerable. More users, a broader network, would invite the hackers to test their skills. Increased use of IoT requires a secured transmission.

In most of the encrypted transmissions, a key [13-15] is passed to be deciphered at the receiver's end. If one breaks the key one can hack the network easily. A keyless encryption technique is the solution which would make it almost impossible to decipher or hack the system.

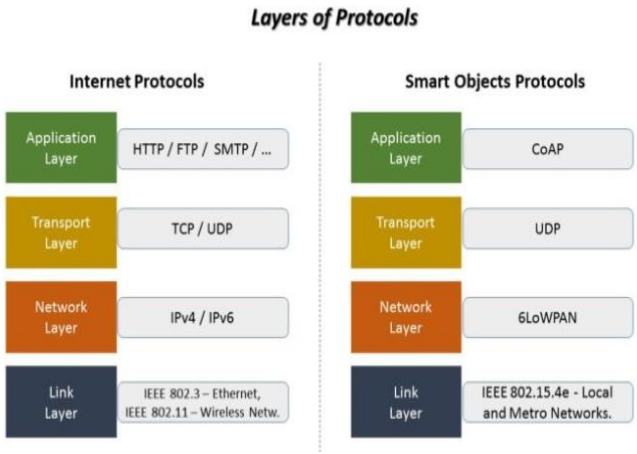

Fig. 1 Shows the different IoT networks [16]

Figure 1. shows different services which can be considered for IoT. The attacks like MiTM, DDoS have been shown. The figure sums up different networks (Smart home, Cellular and healthcare network) and the places where hackers exploit to carry out the attacks.

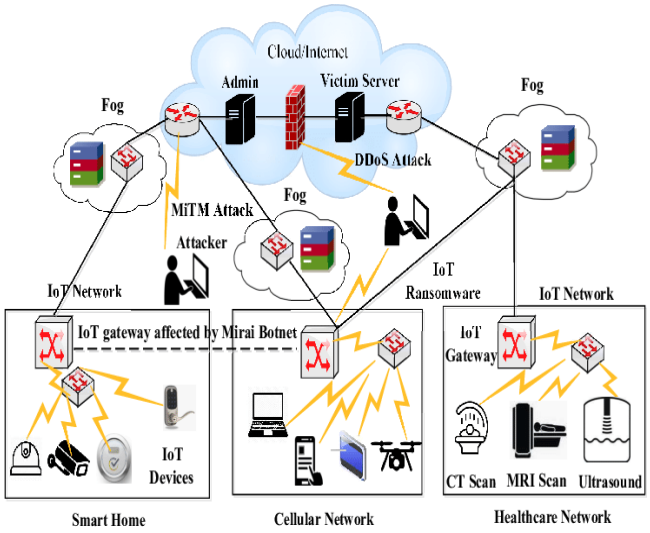

Fig. 2 Comparison of Internet Protocols and Smart object protocols [17]

Figure 2. shows comparison of protocols used in the Internet and Smart devices. In 'Smart Objects Protocol', the network layer shows a Low Power Wireless Personal Area Networks (6LoWPAN) protocol. The principle of IPv6 over 6LoWPAN derives from the belief that "the Internet Protocol can and should be extended to even the smallest devices and low-power machines with minimal computing resources should be able to engage in the IoT".

IoT devices have specific functions and very little room for robust security mechanism as the aim is to extend it to the smallest device. 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 don't even change their default username and password.

Keeping these in mind and looking at the demand of a secured IoT, we propose a unique 3-layer protection model. At the transmission level, group key establishment and device key establishment.

2. Related Work

Li et al in [18] focus on the protection of privacy in Smart Grid buildings. The paper presumes that the key server and the trust centre are always available. But it does not talk about security. Navneet in [19] presented Smart Meter's Secure Key Distribution Protocol which mainly concentrated on preventing man-in-the-middle attack. The paper presents only a security review with no assessment of the results. Luca in [20] proposed Vehicle-to-vehicle communications in ad hoc networks. The paper proposes to carry out batch leave operations based on a predetermined leave period specified by members as they join. The paper assumes that every member is aware of the exact time to leave the party, which is not always the case.

Beside specific applications, different authentication schemes have also been proposed by various researchers. Jang in [21] proposed a scheme "Marker Hash-Tree". It proposed device authentication without involving the central authority. Sharaf in [22] proposed a fingerprinting authentication protocol for IoT devices. It has a transfer learning method which could mitigate emulation attack effectively. Sciancalepore in [23] proposed a key management scheme along with device authentication. The proposed model could handle *fast re-keying*, *replay attack*, and *robust key negotiation.* Li in [24] 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. Braeken in [25] proposed an efficient and distributed authentication protocol for smart homes. The model has a low computation cost,

but the communication cost is high. Luo in [26] 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. Owing to the use of CLC and bilinear matching operations their scheme is therefore expensive in terms of overhead computation.

Xu in [29] suggests a two-factor mutual authentication and a key agreement scheme to minimize computational costs based on elliptic curve cryptography (ECC), which would allow the use of dynamic identity to provide anonymity. Yan in [30] suggested a device verification system based on biometrics. But his scheme is vulnerable to the *replay attack*, and *word guessing attack*. Mishra [31] proposed an enhanced scheme for biometric authentication using random numbers. Tan in [32] expanded the security specifications of two-factor authentication schemes to three-factor authentication systems, which are mutual identification, password and biometric anonymous repositories, and three-factor encryption systems. Guo [33] 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. The scheme does not maintain user privacy and double-secret keys inefficiency. Hao in [34] proposed an improved scheme that could solve Guo's vulnerability. Lee [35] and Jiang [36] improvised [34] the scheme. Chun [36] noticed that both Lee's [35] and Jiang's [36] systems are vulnerable to the assault on service misuse and proposed a stable authentication scheme to fix the security vulnerability. Lu [39] 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 in [39] proposed a three-factor authentication scheme. Moon [37] explained that the scheme of [36] is not safe from *replay attack, impersonation attack, an intruder attack*. They suggest a changed authentication system to correct such security vulnerabilities. Roy in [38] 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.

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. 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 [41-45]. Many schemes [24-26] have a session key security flaw under the new de facto (Cipher Key) CK-adversary model [27, 28]. [46] introduced light weight key management system (KMS). KMS updates the keys which can easily hackers can easily break, the research is more theoretical.

A thorough study motivated the authors to introduce a 3S-IoT model. The model adapts to the dynamic nature of IoT scenarios and provides 3-level security. Each level of security can also be used independently for securing any communication and encrypting the images.

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.

Experimental 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 $\leftarrow$ 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:

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

3.1.1 Explanation of Objective Function

i. First, take a 32X32 image and convert it into a 256-bit binary scalar matrix and then store 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.
ii. 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 given below.
iii. 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.
iv. 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: This image is encrypted using 64-bit encryption, (first objective function). It is called N_k (network key)
Step5: Once we encrypt the image, we delete 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 eq (1)

$$Connection = \begin{cases} 0 \text{ if no match} \\ 1 \text{ if match found} \end{cases} \text{.....eq(1)}$$

Step9: Group key, G_k is created using fn (2)
Step10: Using MD5 generates a Device key D_k. Encrypted image is used for the purpose
Step11: Connection with the device is established if

$$DeviceAccess = \begin{cases} 0 \text{ if no match} \\ 1 \text{ if } G_k \text{ match} \end{cases} and \begin{cases} 0 \text{ if no match} \\ 1 \text{ if } D_k \text{ match} \end{cases} \text{...eq(2)}$$

4. Algorithm for the Proposed Security Model

4.1. Network key establishment using 128-bit image encryption

We propose a unique authentication scheme based on images. We assign 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 recommend taking small images, as IoTs do not have much storage space.

Setup (Encryption at the initiator)

Collect greyscale images
Initialize required variables

Start

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

4.1.1 Network key establishment (with responder)

The required image would already be there at the server
Get the image for the IP and MAC address
Perform step 1 to 7 at the responder
Establish connection applying eq (1)

4.2. Group key establishment

Setup
Initialize required variables
Generate numbers using Machine Learning's Linear Regression
Step 1: Fix Random seed
Step 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
Step 3: predictor ← LinearRegression (number of jobs = -1)
Step 4: output← predictor.fit (Input, Output)
Step 5: Test_set ← Group ID
Step 6: output ← predict Test_set using fn (1)

$$\sum_{n=1}^{100} predictor(T_{input}, T_{output}) \quad \text{.....fn(1)}$$

Here,

n: number of counts

$predictor(T_{input}, T_{output})$: Predicted vaues, Linear Regression

Generate values using Lorenz Map
Step 7. n← 100
Step 8. L← generate Lorenz numbers using the equation in fn (2)

$$\sum_{i=1}^{n} L_{Chaos}(f, P, t) \text{ .....fn(2)}$$

Here,

P: Predcited values

t: hundred random numbers with a step of 0.01

$f: [\sigma \times (p1 - p2), t1 \times (rho - p3), p1 \times p2 - \beta \times p3]$

$\sigma: 10.0$

$rho: 28.0$

$\beta: 8.0/3.0$

Step 9. For several groups:

$G_{k(i)}$ ← assign to a group

End loop

Step 10. Establish group access using eq (2)

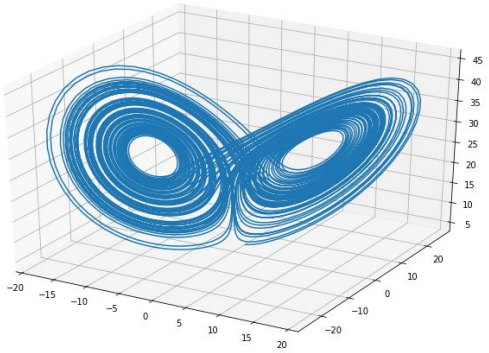

Fig. 3 Lorenz map

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

Setup

Initialize the required variables

Step 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

Step 2: For i 1 to length of V do

Device← V(i)

End for

5. Mathematical Analysis

To check robustness of the proposed algorithm, we have calculated energy consumed, bandwidth consumed, and time utilized.

5.1. Energy Calculation

$$E_c = \frac{\sum_{i=1}^{n}(E - e_i)}{n} \quad \text{..... eq(3)}$$

Here,

E_c is the Energy consumed

E is the total energy

n is the number of sensors

e_i is the energy required

5.2. Bandwidth Calculation

$$bw_c = \frac{\sum_{i=1}^{n}(Bw - bc_i)}{n} \quad \text{..... eq(4)}$$

Here,

bw_c is the Bandwidth consumed

Bw is the total Bandwidth

n is the number of sensors

bc_i is the bandwidth required

5.3. The calculation for Time Taken

$$T_c = \sum_{i=1}^{n}(T_{stop} - T_{start}) \quad \text{..... eq(5)}$$

Here,

T_c is the Time consumed

T_{start} is the start time

T_{stop} is the stop time

n is the number of sensors

6. Authentication Analysis

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.

7. 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.

8. 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 3 to 5 have been used for the calculations.

Table 1 Comparison with previous related work

Security Attribute	[3]	Moon[37]	Roy[38]	Xu[40]	Liu[42]	Das[47]	Proposed
Stolen smart card or mobile device attack		Y	Y	Y	Y		Y
Replay attack	Y		Y		Y	Y	Y
Password guessing attack	Y	Y	Y	Y	Y		Y
Privileged insider attack	Y	Y	Y	Y	Y		Y
Known session key secrecy	Y	Y	Y	Y	Y	Y	Y
Session key security	Y	Y	Y	Y	Y	Y	Y
User impersonation attack	Y	Y	Y	Y	Y	Y	Y
Server impersonation attack	Y	Y	Y	Y	Y	Y	Y
Server-insider attack					Y		Y
Revocation of smart device			Y		Y	Y	Y
Secure mutual authentication	Y	Y	Y	Y	Y		Y
Password remote authenticate					Y	Y	Y
Formal security analysis		Y	Y		Y		Y
Strong secure secret key	Y				Y	Y	Y
Group Key Establishment							Y
Man, in the Middle Attack						Y	Y
Phishing Attack							Y
3-Tier Security							Y
Malicious device deployment						Y	Y
ESL Attack						Y	Y

Table 1 shows a comparison of attacks the proposed model can mitigate.

Table 2 Functionality Comparison

Parameter	Moon[37]	Roy[38]	Xu[40]	Liu[42]	Das[47]	Kaur[49]	proposed
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 [47]. 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 [47].

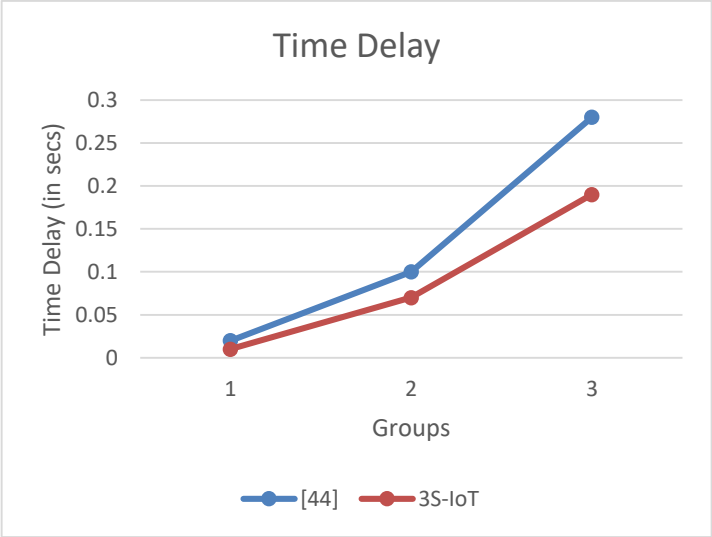

Fig. 4 Time Delay compared with [47]

Figure 4. compares 3s-IoT and [47] on time-delay parameter. As the devices increase in a group the delay increases as well. But, unlike [47] it is not a steep incline in case of 3s-IoT. Also, the delay is less.

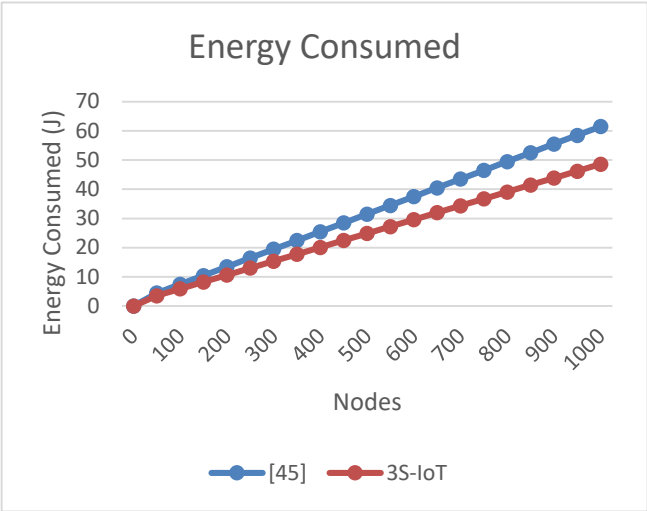

Fig. 5 Energy consumed compared with [48]

It is likely that with an increase in the number of devices, the energy consumption increases. 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 [48] as shown in Figure 5.

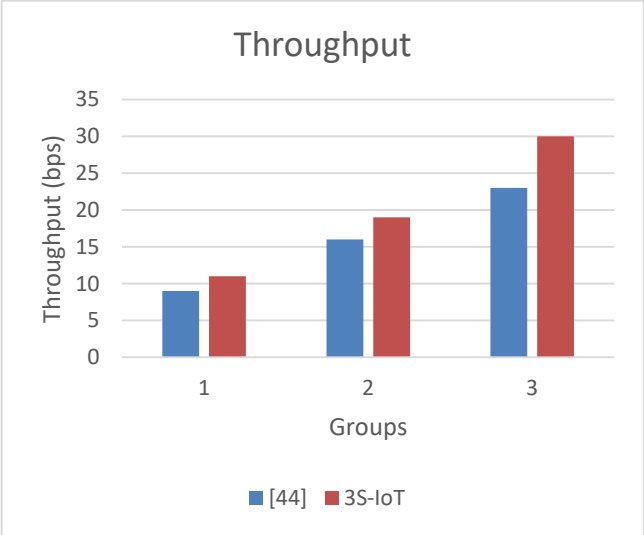

Fig. 6 Throughput compared with [47]

Throughput another very important factor in estimating the cost of a model has been compared with [47] in Figure 6. 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 [47].

8. Conclusion

Our secure IoT architecture provides privacy (through Black Networks), identity manage- ment 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 defense against all kinds of tampering and attacks.

8.1 Highlight

i. The model has three-level security
ii. GK security is based on image encryption. Random numbers could have been used but they can be regenerated. Hackers are smart to understand that random numbers are used.
iii. The model takes only 76 KB space, including the image. This makes it ideal to use with low power consumption devices.
iv. The model can establish the connection very fast.
v. The packet loss is less.
vi. The proposed model can secure any type of network.
vii. The GK algorithm can securely transmit image over any network.

9. Acknowledgement

We want to give thanks to the research facilities provided by College of Engineering Roorkee 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.

References

1. Safaei, A., Monazzah, M., Bafroei, and Ejlali, A. (2017). Reliability side-effects in Internet of Things application layer protocols. *2nd International Conference on System Reliability and Safety (ICSRS)*, 207-212. https://doi.org/10.1109/ICSRS.2017.8272822
2. McKinsey Global Institute. (2015, June). *The Internet of Things: Mapping the value beyond the hype*. Retrieved June 3, 2019 from 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
3. Statista Research Department. (2016, 27 November). *Internet of things (iot) connected devices installed base worldwide from 2015 to 2025.* Retrieved July 12, 2020, *from* https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/
4. United Nations, Department of Economic and Social Affairs, Population Division (2015). *World Population Prospects 2015 – Data Booklet (ST/ESA/SER.A/377)*. Retrieved July 12, 2020 from https://population.un.org/wpp/Publications/Files/WPP2015_DataBooklet.pdf
5. Kambourakis, G., Kolias, C., and Stavrou, A. (2017). The Mirai botnet and the IoT Zombie Armies. *MILCOM IEEE Military Communications Conference (MILCOM), Baltimore, MD*, 267-272. https://doi.org/10.1109/MILCOM.2017.8170867
6. Larson, S. (2017, January 9). *FDA Confirms That St. Jude's Cardiac Devices Can Be Hacked*. CNN Business. Retrieved July 12, 2020 from https://money.cnn.com/2017/01/09/technology/fda-st-jude-cardiac-hack
7. Garlati, C. (2016, October 18). *Owlet Baby Wi-Fi Monitor 'Worst IoT Security Of 2016*. Information Security Buzz. Retrieved July 15,2020 from https://www.informationsecuritybuzz.com/expert-comments/owlet-baby-wi-fi-monitor-worst-iot-security-2016/
8. Cusack, B., & Tian, Z. (2017). Evaluating IP surveillance camera vulnerabilities. *The Proceedings of 15th Australian Information Security Management Conference, 5-6 December.* 25-32. https://doi.org/10.4225/75/5a84efba95b46

9. Thomson, I. (2013, September 5). *FTC slaps TRENDnet with 20 years' probation over webcam spying flaw*. The Register. Retrieved July 15, 2020 from https://www.theregister.co.uk/2013/09/05/ftc_slaps_trendnet_with_20_years_probation_over_webcam_spying_flaw/
10. Greenberg, A. (2013, July 24). *Hackers Reveal Nasty New Car Attacks--With Me Behind The Wheel (Video).* Forbes. Retrieved July 16, 2020 from https://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/?sh=6e1871b9228c
11. Miller, C., & Valasek, C. (2015, August 10). *Remote Exploitation of an Unaltered Passenger Vehicle.* Black Hat USA. Retrieved July 16, 2020 from https://securityzap.com/ files/Remote%20Car%20Hacking.pdf
12. Sivaraman, V., Chan, D., Earl, D., & Boreli, R. (2016). Smart-Phones Attacking Smart-Homes. *Proceedings of the 9th ACM Conference on Security & Privacy in Wireless and Mobile Networks (WiSec '16), Association for Computing Machinery, New York, USA, 195200*. 195-200 https://doi.org/10.1145/2939918.2939925
13. Thomas, M., & Panchami, V. (2015). An encryption protocol for end-to-end secure transmission of SMS. *2015 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2015], Nagercoil.* 1-6. https://doi.org/10.1109/ICCPCT.2015.7159471
14. Zhou, X., and Tang, X. (2011). Research and implementation of RSA algorithm for encryption and decryption. *Proceedings of 6th International Forum on Strategic Technology, Harbin, Heilongjiang*. 1118-1121. https://doi.org/10.1109/IFOST.2011.6021216
15. Bonde, S., & Bhadade, U. (2017). Analysis of Encryption Algorithms (RSA, SRNN and 2 Key Pair) for Information Security. *International Conference on Computing, Communication, Control and Automation (ICCUBEA), Pune*. 1-5. https://doi.org/10.1109/ICCUBEA.2017.8463720
16. Chaudhary, R., Aujla, G.S., Kumar, N., & Zeadally, S. (2019). Lattice-Based Public Key Cryptosystem for Internet of Things Environment: Challenges and Solutions. *IEEE Internet of Things Journal*. 6, 4897-4909. https://doi.org/10.1109/JIOT.2018.2878707
17. The Internet of Things. IoT connectivity – IoT Protocol Layers. Retrieved July 16, 2020 from http://www.infiniteinformationtechnology.com/iot-connectivity-iot-protocol-layers
18. Li D, Zeyar A, Srinivas S, John W, and Abel S. (2013). Privacy Preservation Scheme for Multicast Communications in Smart Buildings of the Smart Grid. *Journal, Smart Grid and Renewable Energy (SGRE)*, 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. (2013). A novel batch-based group key management protocol applied to the Internet of Things. *Elsevier Journal, Ad Hoc Networks,* 11, 2724-2737. http://dx.doi.org/10.1016/j.adhoc.2013.05.009
21. Jang, S., Lim, D., & Kang, J. (2016). An Efficient Device Authentication Protocol without Certification Authority for Internet of Things. In: *Wireless Personnal Communication.* 91, 1681–1695. https://doi.org/10.1007/s11277-016-3355-0
22. Sharaf-Dabbagh, Y. & Saad, W. (2016). On the authentication of devices in the Internet of things. *IEEE 17th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM)*. 1-3. https://doi.org/10.1109/WoWMoM.2016.7523532
23. Sciancalepore, S., Piro, G., Boggia, G., and Bianchi, G. (2017). Public Key Authentication and Key Agreement in IoT Devices with Minimal Airtime Consumption. *IEEE Embedded Systems Letters*. 9: 1-4. https://doi.org/10.1109/LES.2016.2630729
24. Li, F., Han, Y., & Jin, C. (2016). Practical access control for sensor networks in the context of the Internet of Things. *Computer Communications*, 89-90, 154-164. https://doi.org/10.1016/j.comcom.2016.03.007
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*, 12,1-11. https://doi.org/10.1177/1550147716682037
26. Luo, M., Luo, Y., Wan, Y., & Wang, Z. (2018). Secure and efficient access control scheme for wireless sensor networks in the cross-domain context of the IoT. *Security and Communication Networks*, 1-10. https://doi.org/10.1155/2018/6140978
27. Canetti, & Krawczyk, H. (2002). Universally composable notions of key exchange and secure channels. *Proceedings of International Conference on the Theory and Application of Cryptographic Techniques, Amsterdam, The Netherlands,* 337-351. https://doi.org/10.1007/3-540-46035-7_22
28. Abdalla, M., Fouque, P., & Pointcheval, D. (2005). Password-based authenticated key exchange in the three-party setting. *Springer, Berlin, Heidelberg, Public Key Cryptography,* 3386,65-84. https://doi.org/10.1007/978-3-540-30580-4_6
29. Xu, X., Zhu, P., Wen, Q., Jin, Z., Zhang, H., & He, L. (2014). A Secure and Efficient Authentication and Key Agreement Scheme Based on ECC for Telecare Medicine Information Systems. In: *Journal of Medical System*. 38, 9994. https://doi.org/10.1007/s10916-013-9994-8
30. Yan, X., Li, W., Li, P., Wang, J., Hao, X., & Gong, P. (2013). A Secure Biometrics-based Authentication Scheme for Telecare Medicine Information Systems. *Journal of Medical Systems*, 37, 1-6. https://doi.org/10.1007/s10916-013-9972-1

31. Mishra, D., Mukhopadhyay, S., Kumari, S., Khan, M. K., & Chaturvedi, A. (2014). Security enhancement of a biometric based authentication scheme for telecare medicine information systems with nonce. *Journal of Medical System* 38(5),41. https://doi.org/10.1007/s10916-014-0041-1
32. Tan, Z. (2014). A User Anonymity Preserving Three-Factor Authentication Scheme for Telecare Medicine Information Systems. Journal of Medical Systems 38(3):16. https://doi.org/10.1007/s10916-014-0016-2
33. Guo, C., & Chang, C. C. (2013). Chaotic maps-based password authenticated key agreement using smart cards. *Communications in Nonlinear Science and Numerical Simulation,* 18, 1433-1440. https://doi.org/10.1016/j.cnsns.2012.09.032
34. Lee, T. (2013). An Efficient Chaotic Maps-Based Authentication and Key Agreement Scheme Using Smartcards for Telecare Medicine Information Systems. *Journal of Medical Systems,* 37;9986. https://doi.org/10.1007/s10916-013-9985-9
35. Jiang, Q., Ma, J., Lu, X., & Tian, Y. (2014). Robust Chaotic Map-based Authentication and Key Agreement Scheme with Strong Anonymity for Telecare Medicine Information Systems. *Journal of Medical Systems,* 38. https://doi.org/10.1007/s10916-014-0012-6
36. Hao, X., Wang, J., Yang, Q., Yan, X., & Li, P. (2013). A Chaotic Map-based Authentication Scheme for Telecare Medicine Information Systems. *Journal of Medical Systems,* 37. https://doi.org/10.1007/s10916-012-9919-y
37. Moon, J., Choi, Y., Kim, J., & Won, D. (2016). An Improvement of Robust and Efficient Biometrics Based Password Authentication Scheme for Telecare Medicine Information Systems Using Extended Chaotic Maps. *Journal of Medical Systems,* 70. https://doi.org/10.1007/s10916-015-0422-0
38. Roy, S., Chatterjee, S., Das, A. K., Chattopadhyay, S., Kumari, S., & Jo, M. (2018). Chaotic Map-Based Anonymous User Authentication Scheme With User Biometrics and Fuzzy Extractor for Crowdsourcing Internet of Things. *IEEE Internet of Things Journal,* 5, 2884-2895. https://doi.org/10.1109/JIOT.2017.2714179.
39. Lu, Y., Li, L., Pengand, H., & Yang, Y. (2016). A secure and efficient mutual authentication scheme for session initiation protocol. *Peer-to-Peer Networking and Application*, 9,449-459. https://doi.org/10.1007/s12083-015-0363-x
40. Xu, X., Zhu, P., & Wen, Q. (2014). A Secure and Efficient Authentication and Key Agreement Scheme Based on ECC for Telecare Medicine Information Systems. *Journal of Medical Systems*, 38,9994.
41. Chain, K., Chang, K. H., Kuo, W. C. and Yang, J. F. (2018). Enhancement authentication protocol using zero-knowledge proofs and chaotic maps: ENHANCEMENT AUTHENTICATION PROTOCOL. *International Journal of Communication System*, 30. https://doi.org/10.1002/dac.2945
42. Liu, W., Wang, X., and Peng, W. (2020). Secure Remote Multi-Factor Authentication Scheme Based on Chaotic Map Zero-Knowledge Proof for Crowdsourcing Internet of Things. *IEEE Access*, 8, 8754-8767. https://doi.org/10.1109/ACCESS.2019.2962912
43. Xie, Q., Liu, W., Wang, S., and Han, L. (2014). Improvement of a Uniqueness-and-Anonymity-Preserving User Authentication Scheme for Connected Health Care. *Journal of Medical Systems*, 38. https://doi.org/10.1007/s10916-014-0091-4
44. Xu, L. D., He, W., and Li, S. (2014). Internet of Things in Industries: A Survey. *IEEE Transactions on Industrial Informatics*, 10, 2233-2243. https://doi.org/10.1109/TII.2014.2300753
45. Lee, C., Lin, T. H., & Chang, R., X. (2011). A secure dynamic ID based remote user authentication scheme for multi-server environment using smart cards. *Expert Systems with Applications,* 38, 13863-13870. https://doi.org/10.1016/j.eswa.2011.04.190
46. Duan, L., Li, Y., & Liao, L. (2020). 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. https://doi.org/10.1145/3410992.3411006
47. Das, A. K., Wazid, M., Yannam, A. R., Rodrigues, J., & Park, Y. (2019). Provably Secure ECC-Based Device Access Control and Key Agreement Protocol for IoT Environment. *IEEE Access*, 7, 55382-55397. https://doi.org/10.1109/ACCESS.2019.2912998
48. Gu, H., & Potkonjak, M. (2018). Efficient and secure group key management in IoT using multistage interconnected PUF. *Proceedings of the International Symposium on Low Power Electronics and Design,* 8, 1-6.
49. Kaur, R., Kaur, N., & Sood, S. K. (2017). Security in IoT network based on stochastic game net model. In: *International Journal of Network Mgmt*, 27. https://doi.org/10.1002/nem.1975

Figures

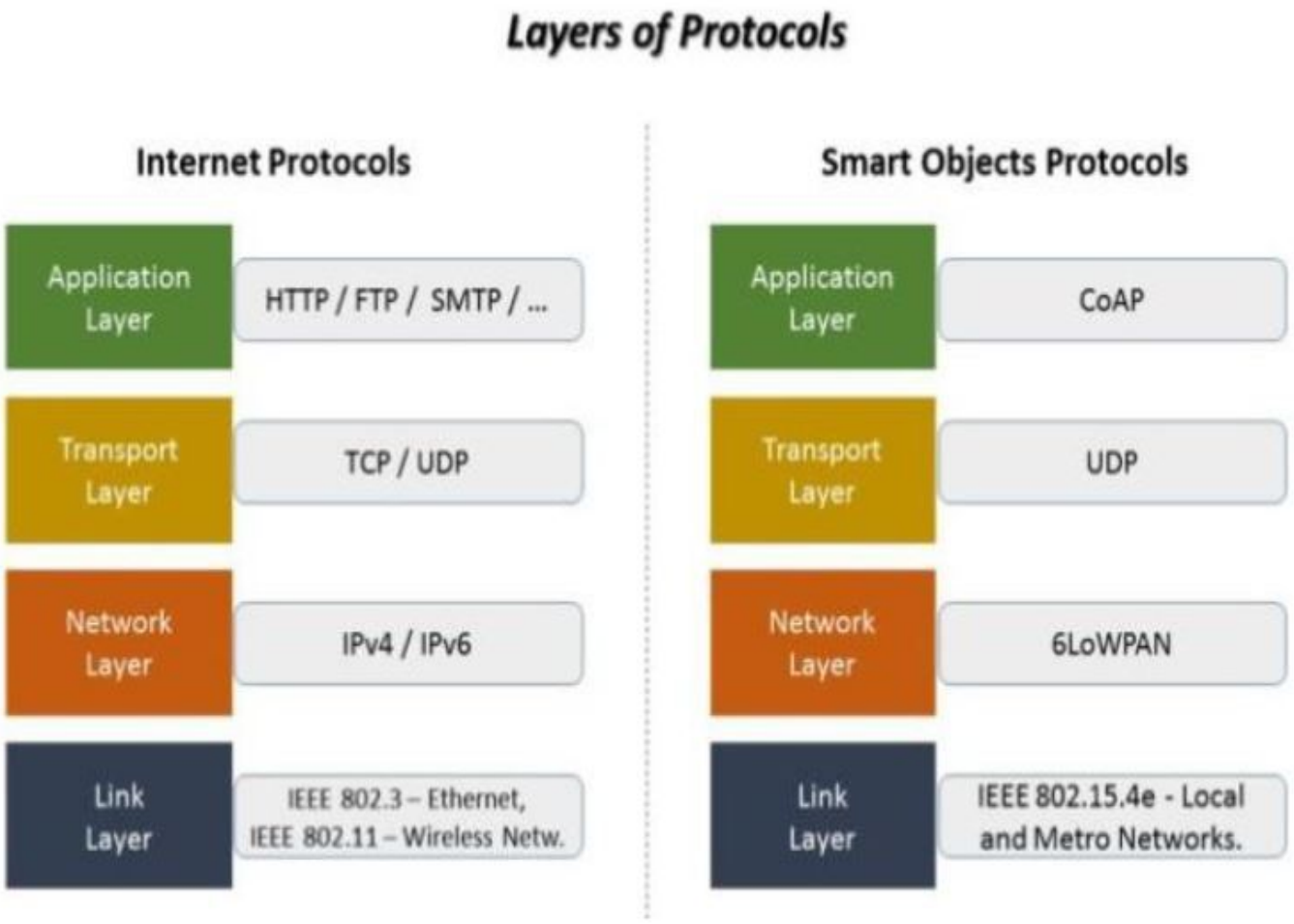

Figure 1

Shows the different IoT networks [16]

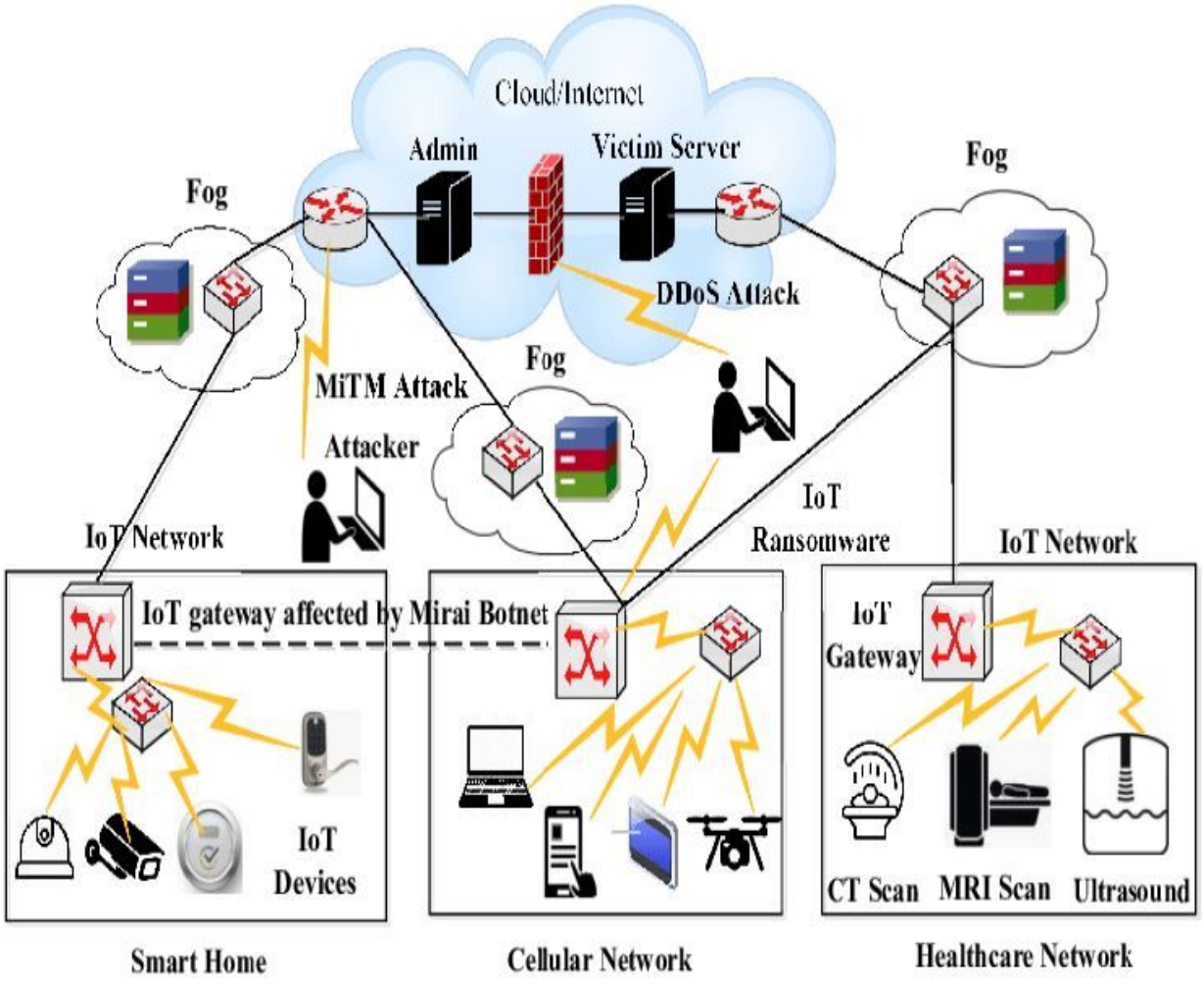

Figure 2

Comparison of Internet Protocols and Smart object protocols [17]

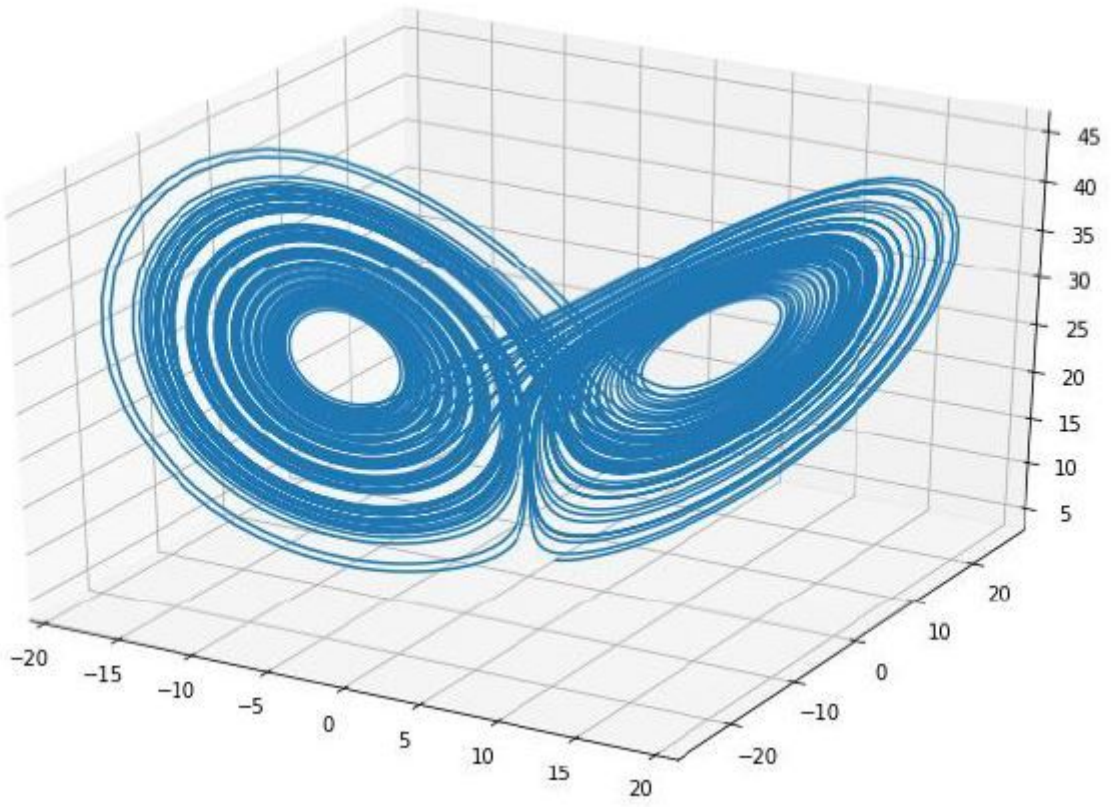

Figure 3

Lorenz map

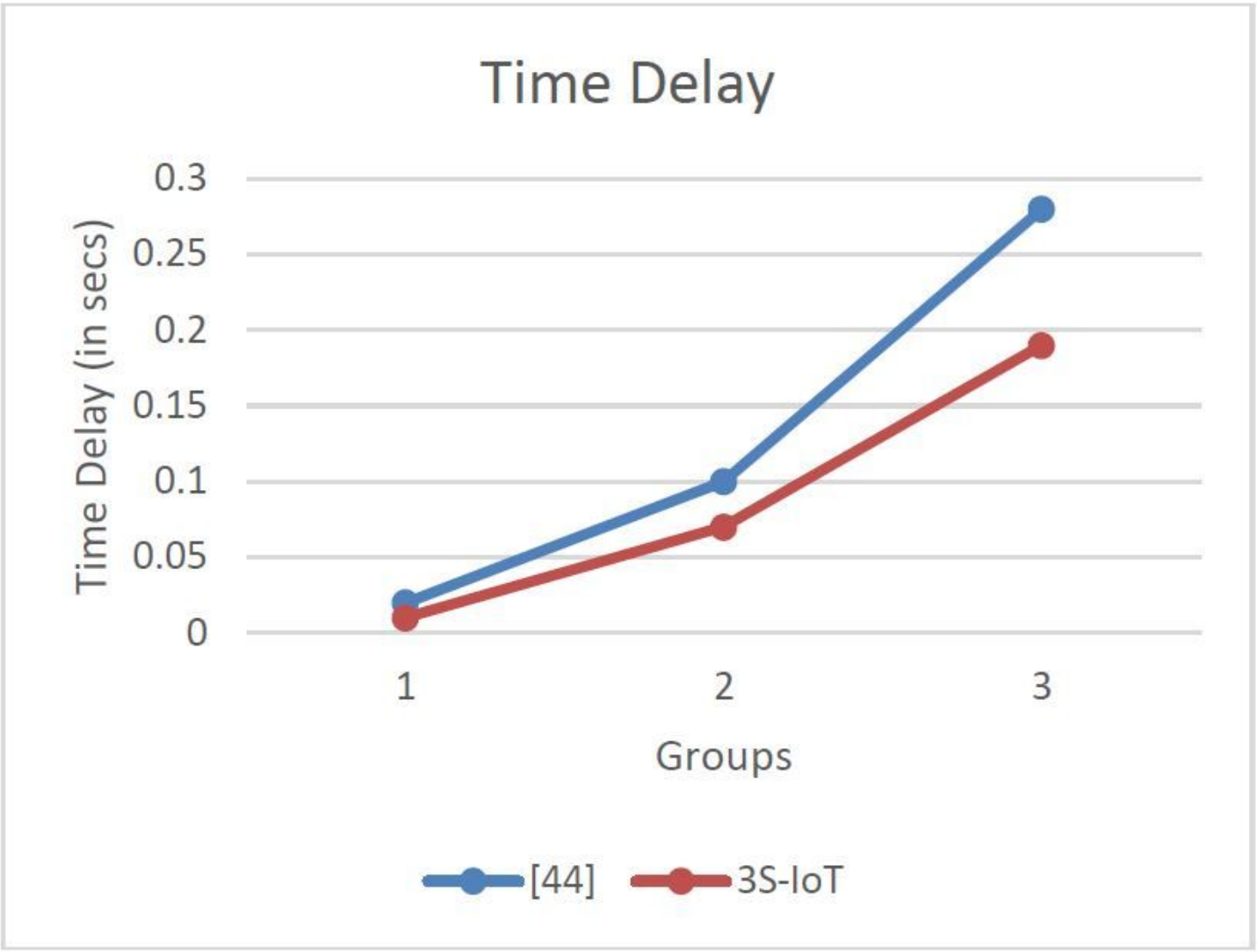

Figure 4

Time Delay compared with [47]

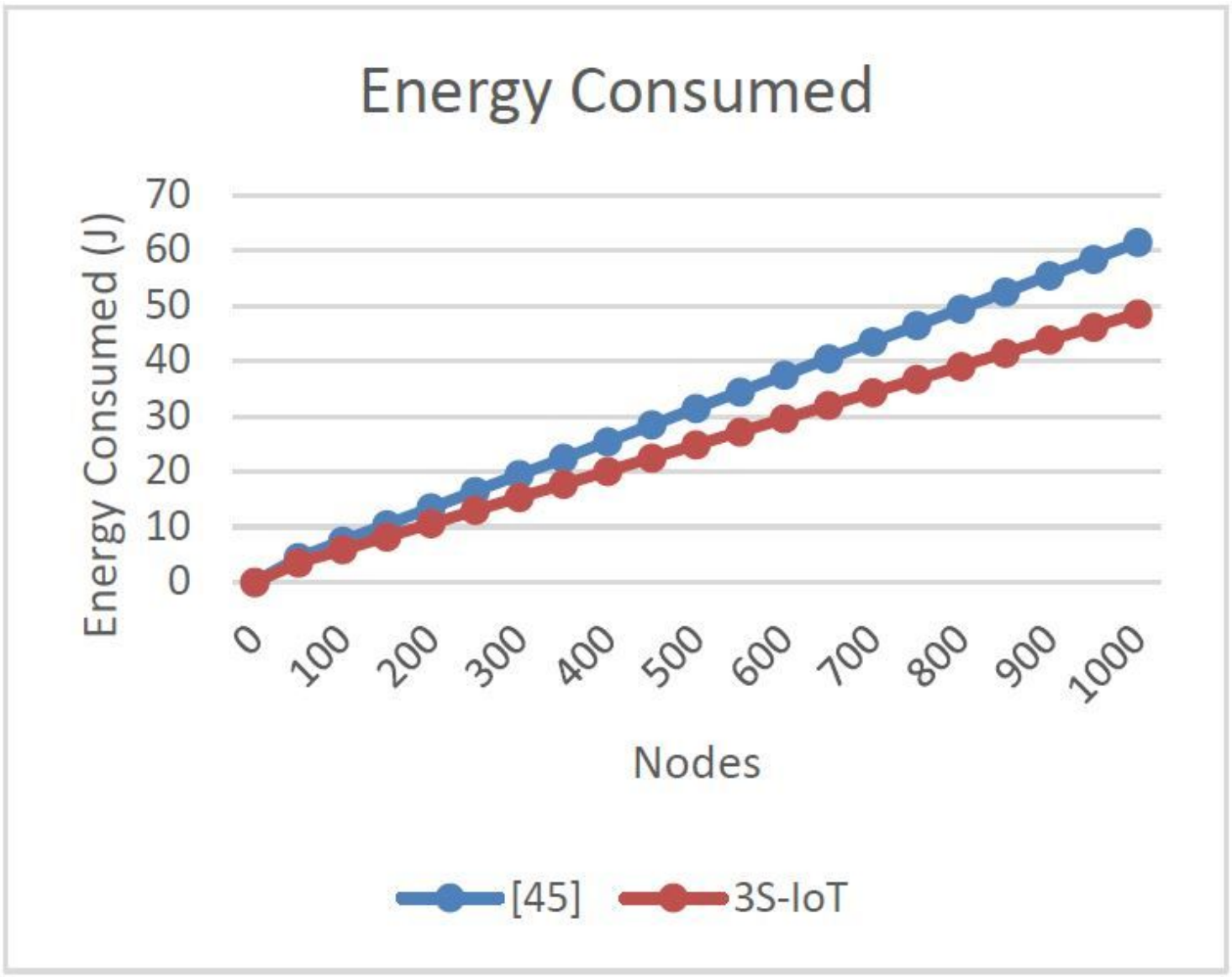

Figure 5

Energy consumed compared with [48]

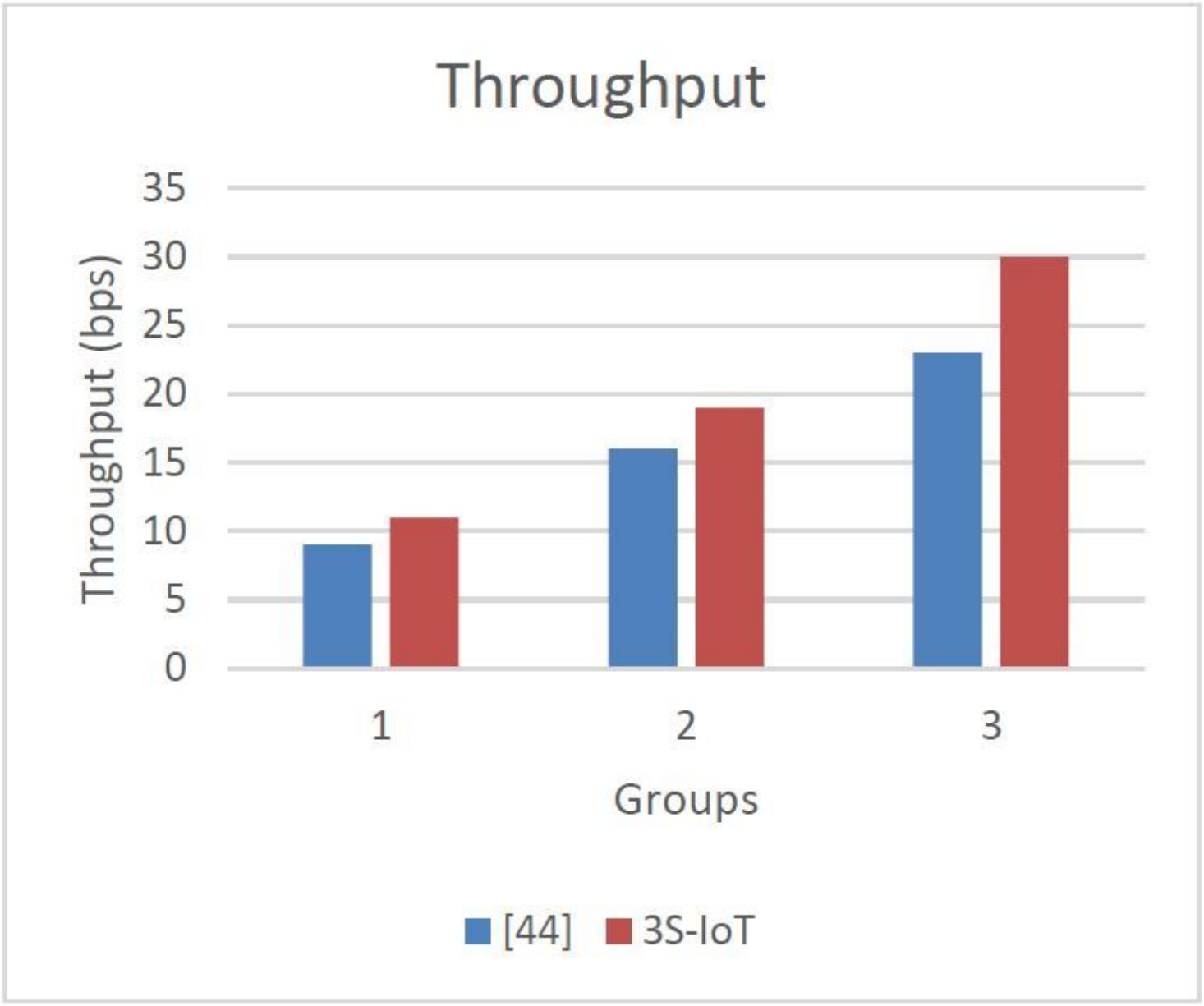

Figure 6

Throughput compared with [47]

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- AuthorsPictureBiography.pdf