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

Maneesh Pant (maneeshgbpuat@gmail.com)
College of Engineering Roorkee
Brij Mohan 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: November 6th, 2020

DOI: https://doi.org/10.21203/rs.3.rs-92971/v1

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

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

[1]Department of Computer Science and Engineering, Research Scholar Uttrakhand University Dehradun, Uttrakhand, India
[2] Department of Computer Science and Engineering, College of Engineering Roorkee, Roorkee, Uttrakhand, India
[3] Department of Mathematics, College of Engineering Roorkee, Roorkee, Uttrakhand, India
[*]maneeshgbpuat@gmail.com

Abstract: Internet of Things (IoT) evolving and widespread presence has made the lives of all comfortable and handy, while on the other hand posing various challenges, i.e. less efficiency, less security, and high energy drain, threatening smart IoT-based applications. Compared to unicast communication, multicast communication is considered more powerful in group-oriented systems, because transmission takes place using less resources. This is why many of the IoT applications rely on multicast in their transmission. This multicast traffic needs to be handled explicitly for sensitive applications requiring actuator control. Securing multicast traffic by itself is cumbersome as it requires an efficient and flexible Group Key Establishment (GKE) protocol. We propose a three-tier model that can, not only be used to control the IoT, but also to control multicast communications. The architecture is built with a 256-bit keyless encryption technique to protect the authentication to create the network link. Machine learning-based chaotic map key generation is used to protect GKE. Finally, using MD5, the system key is authenticated. The algorithm is checked for energy used, bandwidth, and time taken. The proposed model is applied and evaluated against numerous benchmark attacks such as Distributed Denial of Service (DDoS), Man in the Middle and Fishing.

Keywords: IoT devices, smart devices, secured IoT, secured group key, secured network key, secured device key

1. Introduction

IoT is the technology which hackers look at with greedy eyes. Internet means network of networks and network means vulnerability. The networks are prone to attacks and DDoS is the most common of them. IoT connectivity for homes is very simple these days. One can simply connect the devices, for example, ACs of a house using IoT switches like sonoff and control them through a mobile phone. IoT switches are configured using an App but the catch is the switch connects the device to the provider's cloud or a dedicated server, which obviously is on the internet and then the instructions are transmitted to the device. One can imagine, how vulnerable it can be. This means one needs a secured server even for a small connection. Secured servers like AWS are secured but very costly. How can a switch like sonoff, available at 400 Rupees be able to secure the costly servers? Our CCTVs at home and offices are connected over the cloud too. The server is again provided by the vendor of the cameras, which is not very secure. To check the vulnerability of Cameras one can go to Google Dorks and easily find open cameras. Which obviously can be easily hacked. 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]. More users, wider network, would invite the hackers to test their skills. With the wider use of IoT it is important to secure the network.

Malware is one of the favourite tools of hackers. Hacking IoT using it came up in 2016. Mirai IoT Botnet [5] was used to find devices that were still using factory default Username and Password. These systems were hacked using malware. Medical devices use IoT a lot. Cardiac devices from St. Jude were hacked [6], they hacked the devices by accessing their transmitter. Even Owlet WiFi baby [7] heart monitor smart devices were hacked using the same vulnerability. Research [8] has shown that CCTV surveillance devices have vulnerable points. The study showed that over 100,000 wireless Internet Protocol (IP) cameras provided little to no protection. TRENDnet webcam [9], was found to be secured transmitting user's login and password over the internet in simple text and even their mobile application kept the consumer details the same way. The cars we drive these days are vulnerable too to such attacks. Jeep SUV was hacked using CAN bus [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 get a cheap and unsecured device, lethargic to change the factory set username password helps the hackers to attack. Next time when you talk to Alexa make sure it is Alexa. 100 Million home gadgets are vulnerable [12]. Even the transmission can be hacked, the information has to be neatly secured.

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

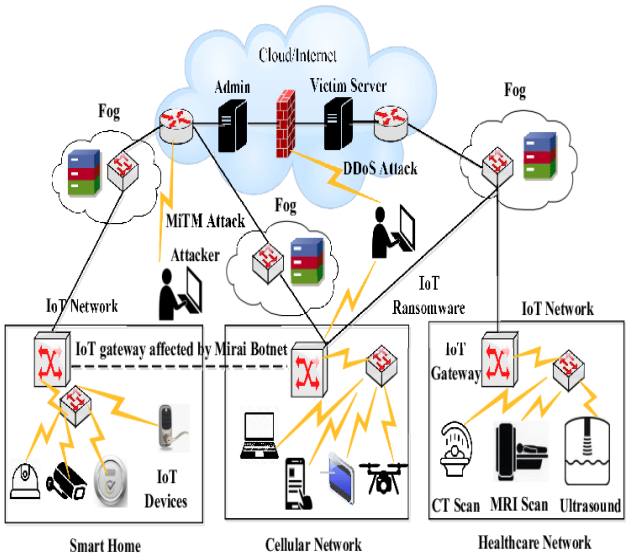

Fig. 1. Shows the different IoT networks [16]

Fig. 1. shows different services which can be considered for IoT [16]. The attacks like Man in the middle (MiTM), DDOS have been shown. The figure sums up the network and the places the hackers exploit to carry out the attacks.

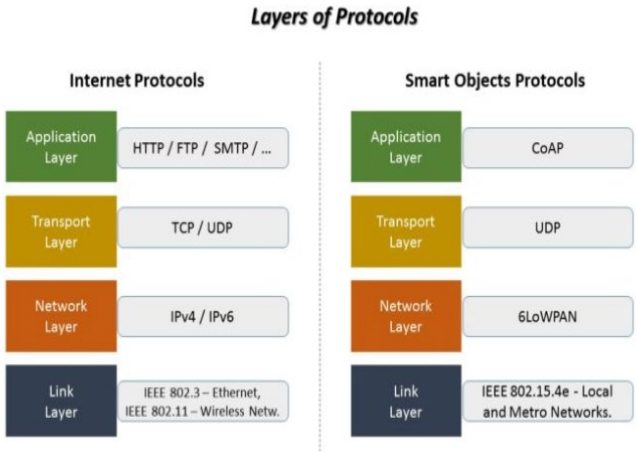

Fig. 2. Comparison of Internet and Smart object protocol (http://www.infiniteinformationtechnology.com/iot-connectivity-iot-protocol-layers)

Fig. 2. shows a comparison of protocols used in Internet and Smart devices. The network layer shows Low Power Wireless Personal Area Networks (6LoWPAN). 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 that low-power machines with minimal computing resources should be able to engage in the Internet of Things.

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 for a standard 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 a unique security system has been designed. The system has three levels of security. At the transmission level, group key establishment and device key establishment. Various attacks have also been tried and quality of the image transmitted has also been tested to check the quality of the service and robustness of the system.

2. Similar Work

This section of the paper briefly describes the IoT network and the protocol considered. It is followed by Objective functions, steps, and pseudocodes to understand the working.

The researchers have focused mostly on rekying protocol or very specific to an application [40-44]. Li et al in [17] focuses on the protection of privacy in Smart Grid buildings. The paper presumes that the key server and the trust centre are always available. It does not state anything about security. Navneet in [18] presented Smart Meter's Secure Key Distribution Protocol. Mainly concentrated on preventing man-in-the-middle attacks. The paper presents only a security review with no assessment of the results. Luca in [19] Vehicle-to-vehicle communications in vehicle ad hoc networks is proposed. The paper proposes that batch leave operations be conducted on the basis of a predetermined leave period specified by members as they join. The paper assumes 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 [20] proposed a scheme "Marker Hash-Tree". It proposed device authentication without involving the central authority. Sharaf in [21] proposed a fingerprinting authentication protocol for IoT devices. It has transfer learning method which could mitigate emulation attack effectively. Sciancalepore in [22] 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 [23] 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 therefore expensive in terms of overhead computation. Braeken in [24] proposed an efficient and distributed authentication protocol for smart homes. The model has low computation cost, but the communication cost is high. Luo in [25] suggested "an IoT cross-domain efficient access control protocol for WSNs that 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 [28] suggested 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 [29] suggested a device verification system based on biometrics. But his scheme is vulnerable to the replay attack, and word guessing attack. It cannot provide protection for users. Mishra [30] proposed an enhanced scheme for biometric authentication using random numbers.

Tan in [31] 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 [32] 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 [33] proposed improved scheme that would solve Guo's vulnerability. Lee [34] and Jiang [35] improvised [33] scheme. Chun [35] notices that both Lee's [34] and Jiang's [35] systems are vulnerable to the assault on service misuse and have a stable authentication scheme to fix the security vulnerability. Lu et. al. 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 [38] proposed a three-factor authentication scheme. Moon [36] finds that the scheme of [35] is not safe from replay attack, impersonation attack, and intruder attack. They suggest a changed authentication system to correct such security vulnerabilities. Roy in [37] claimed that the current 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. In addition, those researches work on just one or two aspects of IoT assuming that the conditions of the application scenario is static which is not the case for IoT application scenarios which have dynamic and varying nature regarding the network access technology, type of application, state of members and key servers and the load on them. Many schemes [23-25] have a session key security flaw under the new de facto (Cipher Key) CK-adversary model [26, 27]. This motivated to introduce 3S-IoT model that adapts to the dynamic nature of IoT scenarios and provides 3-level security.

3. Methodology

The paper aims at providing a three-tier safety to IoT. The main objective function mathematical represents the objectives of 3S-IoT.

3.1. Objective function

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

There are three main objectives of the proposed model, establish secured network connection, access group key and then access device securely.

3.1.1. Explanation

i. Convert a 32X32 image into 256-bit binary scalar matrix, Store it on target network ID

$$\sum_{\forall I} L(B_{256}(\mathrm{I})) \quad \text{..... fn(1)}$$

Here,

$\forall I$: All the elements of image I

$L(B_{1024}(\mathrm{I}))$: 256 bit encrypted image

ii. Using Lorenz system generate a sequence of 100 numbers from predicted 9-digit target ID using Machine Learning's linear regression.

$$\sum_{n=1}^{100} predictor(T_{input}, T_{output}) \text{ .....fn(2)}$$

Here,

n : number of counts

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

$$\sum_{i=1}^{n} L_{Chaos}(f,P,t) \text{ .....fn(2.1)}$$

Here,

f :

P : Predcited values

t : hnundred random numbers with a step of 0.01

$L_{Chaos}(f,P,t) : \left[\sigma \times (p1 - p2), t1 \times (rho - p3), p1 \times p2 - \beta \times p3\right]$

σ :10.0

rho : 28.0

β : 8.0 / 3.0

iii. Generate MD5 of sequence generated of the image

$$\sum_{\forall I} MD_5(I) \text{ ..... fn(3)}$$

Here,

$\forall I$: All the elements of the Image

The methodology adopted is summarized in following steps:

3.2. Setup for Testing

Power←1 Mw
BW ← 256 kbps
Protocol ← 6LowPAN
Packets ← IPv6 (6LowPAN is used to send IPv6 packets over IEEE802.15.4)
Network Protocol ← IEEE802.15.4
Packet size ← 127 octets

3.2.1. Steps

Step1: Initiator and responder are created and assigned cloud ID.

Step2: The initiator creates a multicast group MG = G1, G2….Gn-1 and generate separated Gk IDs.
Step3. An image is assigned to initiator. Images are 32X32. Same is stored at the responder.
Step4. This image is encrypted using a 64-bit encryption, (first objective function). It is called Nk (network key)
Step5: Once image is encrypted the original image at the initiator is deleted.
Step6: Convert the image to scalar
Step6: To establish connection initiator passes Nk to the responder.
Step7. Responder first reshapes the scalar matrix then, decrypts Nk and matches with the stored image. A connection is established using eq (1)

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

Step8: Group key, Gk is created using fn (2).
Step9: Using MD5 generate a Device key Dk. Encrypted image is used for the purpose
Step10: Connection with the device is established if

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

4. Pseudocodes

4.1. Network key establishment 128-bit image encryption

The paper proposes a unique method where an image is used as the access key to the network. Each image is assigned to establish the network. A smart home network would have a unique key, a hospital different, and traffic system different. Each application would have a unique network key. For the experimental purpose 32X32 grey scale images have been considered, though the code is not limited to the size of the image.

Setup (Encryption at the initiator)

Collect grey scale images
Initialize required variables

Start

Step 1. I ← read grey scale image
Step 2. [r, c] ← size(I)
Step 3. I ← I/256 # convert to binary
Step 3. Rs← fix random seed with device id
Step 4. bn ←generate a set of [r x c] binary, random numbers
Step 5. Ie ← replace least significant bit of I with bn
Step 6. It ← reshape Ie to (r x n) scalar matrix

4.1.1. Network key establishment (with responder)

Required image would already be there at the server
Get the image for the IP and MAC address
Perform step 1 to 6 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

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

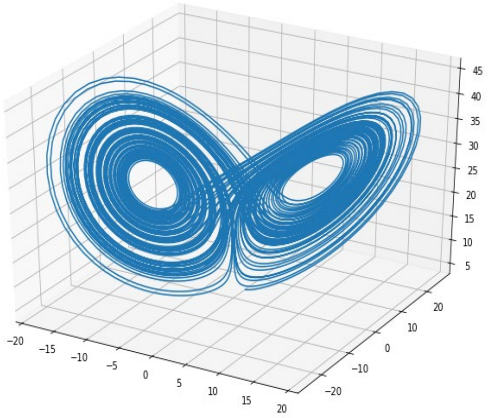

Fig. 3. Lorenz map

Step 9. For number of groups:
Gk(i) ← assign to a group
End loop
Step 10. Establish group access using eq (2)

4.3. Device Key generation and establishment

Setup
Initialize the required variables

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

5. Mathematical Analysis

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. 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

The proposed work does not have any key to decipher. It is purely based on the algorithm designed. The following section describes some of the attacks and how 3S-IoT mitigates them. They key security features are –

a. One to one access only. For example, CCTV's DVR's Mac address, Device ID are stored in the cloud server. When a mobile phone is authenticated the details in encrypted form are stored in the cloud server. Phone number, IP, MAC and authentication details cannot be accessed, or rest once connected. The user has to logout of the mobile device to establish another connection.
b. OTP Authentication required for setup on a mobile
c. Factory set ID and password s 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 first time setup there is no way a password can be changed unless the device is manually reset.
d. Once the user has the access to the device. Network key, Group Key, and Device keys are established.

6.1 Experimental Setup

A smart home network is setup using CCTV cameras, smart ACs, and, Lights. The three groups are integrated over cloud and connected to a Wi-Fi router with an ISP. To access the network over cloud, Redmi Note 9 pro max is used. The required application is installed on the smart phone. 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.

6.2 Attacks

1) Replay Attack, 2) Password guessing attack, 3) Stolen Verifier Attack, 4) Stolen Smart Card or Mobile Device Attack, 5) Privileged insider attack, 6) Known session key secrecy, 7) User impersonation attack, 8) Server impersonation attack, 9) Server-Insider Attack, 10) Man-in-the Middle Attack, 11) Strong secure secret key, 12) Phishing Attack, 13) Botnet, 14) Denial of Service Attack ,15) Trojan

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 connection and that too in encrypted form. Moreover, the images are transmitted in a linear form.

One might argue that Trojan could break the code, but that was taken care of as well. Even when the entire system could be breached, 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. Everything that 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 is able to 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. Results

The work in the paper is simulated using Matlab. The parameters considered for the robustness are - Power consumed, time consumed, and bandwidth required. Equations 3 to 5 have been used for the calculations.

Table 1: Comparison with previous related work

Security Attribute	[39]	[36]	[3]	[37]	[41]	[45]	Proposed
Stolen smart card or mobile device attack	Y	Y	N	Y	Y	N	Y
Replay attack	N	N	Y	Y	Y	Y	Y
Password guessing attack	Y	Y	Y	Y	Y	N	Y
Privileged insider attack	Y	Y	Y	Y	Y	N	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	N	N	N	N	Y	N	Y
Revocation of smart device	N	N	N	Y	Y	Y	Y
Secure mutual authentication	Y	Y	Y	Y	Y	N	Y
Password remote authenticate	N	N	N	N	Y	Y	Y
Formal security analysis	N	Y	N	Y	Y	N	Y
Strong secure secret key	N	N	Y	N	Y	Y	Y
Group Key Establishment	N	N	N	N	N	N	Y
Man, in the Middle Attack	N	N	N	N	N	Y	Y
Phishing Attack	N	N	N	N	N	N	Y
3-Tier Security	N	N	N	N	N	N	Y
Malicious device deployment	N	N	N	N	N	Y	Y
ESL Attack	N	N	N	N	N	Y	Y

Considering [45] throughput and time delay has been considered and compared. The proposed work focuses on energy consumed as well as it is going to play a decisive role when the network would grow. Higher energy consumption may result in network failure.

The proposed work takes in account devices in group. For the sake of testing and comparison same have been divided into three groups having 5,11, and 17 devices in group 1,2, and 3 respectively [45].

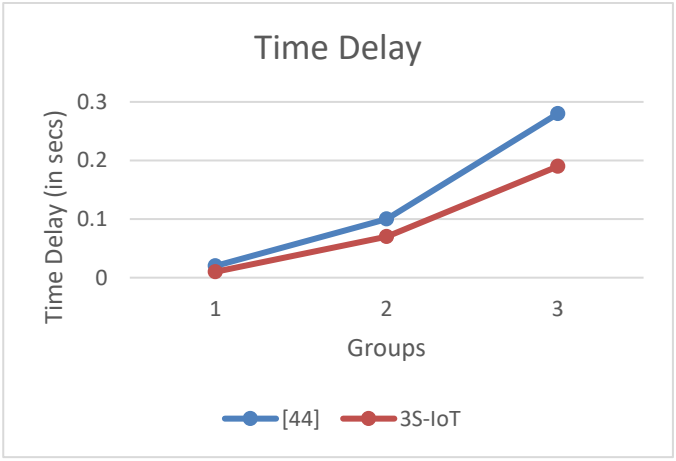

Fig. 4. Time Delay

Fig. 4. compares 3s-IoT and [45] on time-delay parameter. As the devices increase in a group the delay increases as well. But, unlike [45] it is not a steep incline in case of 3s-IoT. Also, the delay is less.

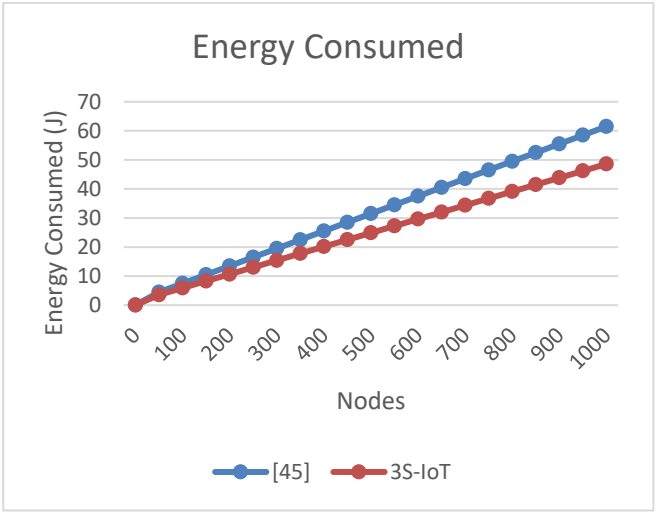

Fig. 5. Energy consumed

It is likely that with an increase in number of devices, the energy consumption increases. The Energy consumed Fig. 5. by 3S-IoT tends to remain constant with the an increase in number of devices. 3S-IoT saves 21% more energy than [46].

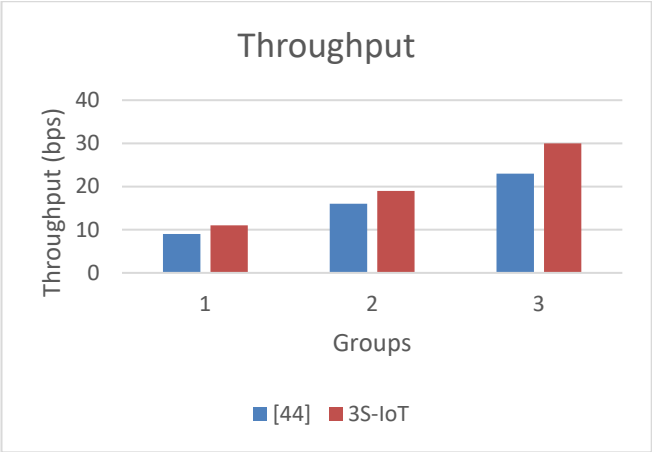

Fig. 6. Throughput

Throughput Fig. 6. another very important factor in estimating the cost of a model has been compared with [45]. The throughput (in bps) increases with an increase in 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 [45].

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 performs relatively well on the three parameters: time, energy, and bandwidth as defined in the results. The proposed work protects the network from known or unknown attacks of all kinds. Since hackers invent almost every day, there is 99 percent 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 is able to install a Trojan, it will only be able to watch but won't be able to manage any device remotely. The model is not 100% protected against Trojan. The attacker can see what is happening, for example it can remotely watch the CCTVs but would not be able to control them. The authors are working on it to make the protection 100 percent. Also, making the sensors temper proof is being considered. The proposed work has hardware security of 80 per cent. The authors are working on cognitive learning to achieve 100 per cent defence against all kinds of tempering and attacks.

8.1. Highlights

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 is able to establish the connection very fast.
v. The packet loss is less.
vi. The proposed model can be used to secure any type of network.
vii. The GK algorithm can be used for secured image transmission

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.

10. References

[1] Safaei, A. M. H. Monazzah, M. B. Bafroei and A. Ejlali, "Reliability side-effects in Internet of Things application layer protocols," in 2nd International Conference on System Reliability and Safety (ICSRS), Milan, 2017, pp. 207-212, doi: 10.1109/ICSRS.2017.8272822.

[2] J. Manyika, M. Chui, P. Bisson, J. Woetzel, R. Dobbs, J. Bughin, and D. Aharon, "The Internet of Things: Mapping the value beyond the hype,", in McKinsey Global Institute. McKinsey, June 2015, p. 3.

[3] Statista Research Department , "Internet of things (iot) connected devices installed base worldwidefrom 2015 to 2025," Accessed: Nov. 27, 2016 [Online], Available: 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) [online]. Available: https://population.un.org/wpp/Publications/Files/WPP2015_DataBooklet.pdf

[5] G. Kambourakis, C. Kolias and A. Stavrou, "The Mirai botnet and the IoT Zombie Armies," in MILCOM 2017 - 2017 IEEE Military Communications Conference (MILCOM), Baltimore, MD, 2017, pp. 267-272, doi: 10.1109/MILCOM.2017.8170867.

[6] S. Larson, "FDA Confirms That St. Jude's Cardiac Devices Can Be Hacked," CNN Money, San Francisco 2017Accessed: Jan. 9, 2017 [Online], Available:https://money.cnn.com/2017/01/09/technology/fda-st-jude-cardiac-hack

[7] C.Garlati, "Owlet Baby Wi-Fi Monitor 'Worst IoT Security Of 2016," Information Security Buzz, 2016Accessed: Oct. 9, 2016 [Online]. Available: https://www.informationsecuritybuzz.com/expert-comments/owlet-baby-wi-fi-monitor-worst-iot-security-2016/

[8] B. Cusack, & Z. Tian,"Evaluating IP surveillance camera vulnerabilities,"inValli, C. (Ed.), The Proceedings of 15th Australian Information Security Management Conference, 5-6 December, 2017, Edith Cowan University, Perth, Western Australia. (pp.25-32), doi: 10.4225/75/5a84efba95b46.

[9] I. Thomson, "FTC slaps TRENDnet with 20 years' probation over webcam spying flaw,"The Register, 2016 Accessed: Sep. 5, 2013 [Online]. Available::https://www.theregister.co.uk/2013/09/05/ftc_slaps_trendnet_with_20_years_probation_over_webcam_spying_flaw/

[10] A. Greenberg, "Hackers Reveal Nasty New Car Attacks--With Me Behind The Wheel (Video)," Forbes, 2020 Accessed: Jul. 24, 2013 [Online]. Available:https://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/#6e3d4bdf228c.

[11] C. Miller and C. Valasek, "Remote Exploitation of an Unaltered Passenger Vehicle," Black Hat USA, 2015Accessed: Aug. 10, 2015 [Online] Available:: https://securityzap.com/files/Remote%20Car%20Hacking.pdf.

[12] V. Sivaraman, D. Chan, D. Earl, and R.Boreli,"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, NY, USA, 195200.DOI:https://doi.org/10.1145/2939918.2939925.

[13] M. Thomas and V. Panchami, "An encryption protocol for end-to-end secure transmission of SMS," in 2015 International Conference on Circuits, Power and Computing Technologies [ICCPCT-2015], Nagercoil, 2015, pp. 1-6, doi: 10.1109/ICCPCT.2015.7159471.

[14] Xin Zhou and Xiaofei Tang, "Research and implementation of RSA algorithm for encryption and decryption," in Proceedings of 2011 6th International Forum on Strategic Technology, Harbin, Heilongjiang, 2011, pp. 1118-1121, doi: 10.1109/IFOST.2011.6021216.

[15] S. Y. Bonde and U. S. Bhadade, "Analysis of Encryption Algorithms (RSA, SRNN and 2 Key Pair) for Information Security," in 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA), Pune, 2017, pp. 1-5, doi: 10.1109/ICCUBEA.2017.8463720.

[16] R. Chaudhary, G. S. Aujla, N. Kumar and S. Zeadally, "Lattice-Based Public Key Cryptosystem for Internet of Things Environment: Challenges and Solutions," in *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4897-4909, June 2019, doi: 10.1109/JIOT.2018.2878707.

[17] D. Li, A. Zeyar, S. Srinivas, W. John, andS. Abel, "Privacy Preservation Scheme for MulticastCommunications in Smart Buildings of the Smart Grid," In Journal, Smart Grid and Renewable Energy (SGRE), no. 04 (2013): 313–324.

[18] N. Agrawal, "Secure Key Distribution Protocol with Smart Meter," in International Journal of Current Engineering and Technology, Vol.5, No.5, Oct 2015.

[19] L. Veltri, S. Cirani, S. Busanelli and G. Ferrari, "A novel batch-based group key management protocol applied to the Internet of Things," in Elsevier Journal, Ad Hoc Networks, Volume 11, Issue 8, 2013, Pages 2724-2737, ISSN 1570-8705, doi: http://dx.doi.org/10.1016/j.adhoc.2013.05.009

[20] S. Jang, D. Lim and J. Kang, "An Efficient Device AuthenticationProtocolwithout Certification Authority for Internet of Things," in Wireless Pers Commun91, 1681–1695 (2016) https://doi.org/10.1007/s11277-016-3355-0

[21] Y. Sharaf-Dabbagh and W. Saad, "On the authentication of devices in the Internet of things," in 2016 IEEE 17th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM), Coimbra, 2016, pp. 1-3, doi: 10.1109/WoWMoM.2016.7523532.

[22] S. Sciancalepore, G. Piro, G. Boggia and G. Bianchi, "Public Key Authentication and Key Agreement in IoT Devices With Minimal Airtime Consumption," in IEEE Embedded Systems Letters, vol. 9, no. 1, pp. 1-4, March 2017, doi: 10.1109/LES.2016.2630729.

[23] F. Li, Y. Han, and C. Jin, "Practical access control for sensor networksin the context of the Internet of Things," in Computer Communications, vol. 89-90,pp. 154-164, Sep. 2016, doi: 10.1016/j.comcom.2016.03.007.

[24] A.Braeken, P. Porambage, M. Stojmenovic, and L. Lambrinos, "eDAAAS: Efficient distributed anonymous authentication and access in smart homes," in International Journal of Distributed Sensor Network, vol. 12, no. 12, pp. 1-11,Dec.2016, doi: 10.1177/1550147716682037.

[25] M. Luo, Y. Luo, Y. Wan, and Z. Wang, "Secure and efficient access control scheme for wireless sensor networks in the cross-domain context of the IoT," in Security and Communication Networks, vol. 2018, pp. 1-10, Aug. 2018, doi: 10.1155/2018/6140978.

[26] R. Canetti and H. Krawczyk, "Universally composable notions of key exchange and secure channels," in Proceedings of International Conference on the Theory and Application of Cryptographic Techniques, Amsterdam, The Netherlands, 2002, pp. 337-351, doi: https://doi.org/10.1007/3-540-46035-7_22

[27] M. Abdalla, P. Fouque, and D. Pointcheval, "Password-based authenticated key exchange in the three-party setting," in Public Key Cryptography PKC, vol. 3386. Berlin, Germany: Springer, 2005, pp. 65-84,doi: https://doi.org/10.1007/978-3-540-30580-4_6

[28] X. Xu et al.,"A Secure and Efficient Authentication and Key Agreement Scheme Based on ECC for Telecare Medicine Information Systems," in Journal of Medical System 38, 9994 (2014), doi: https5//doi.org/10.1007/s10916-013-9994-8

[29] X. Yan et al., "A Secure Biometrics-based Authentication Scheme for Telecare Medicine Information Systems," in Journal of Medical Systems, 2013, 37, pp. 1-6, doi: 10.1007/s10916-013-9972-1.

[30] D. Mishra, S. Mukhopadhyay, S. Kumari, MK. Khan and A. Chaturvedi, "Security enhancement of a biometric based authentication scheme for telecare medicine information systems with nonce,"inJ Med Syst. 2014;38(5):41, doi:10.1007/s10916-014-0041-1.

[31] Z. Tan, "A User Anonymity Preserving Three-Factor Authentication Scheme for Telecare Medicine Information Systems" in Journal of Medical Systems 38.3(2014):16, doi: 10.1007/s10916-014-0016-2.

[32] C. Guo, and C. C. Chang, "Chaotic maps-based password authenticated key agreement using smart cards," in Communications in Nonlinear Science and Numerical Simulation 18.6(2013), pp.1433-1440,doi: https://doi.org/10.1016/j.cnsns.2012.09.032.

[33] T. Lee, "An Efficient Chaotic Maps-Based Authentication and Key Agreement Scheme Using Smartcards for Telecare Medicine Information Systems," in Journal of Medical Systems 37, 9985 (2013), doi: https://doi.org/10.1007/s10916-013-9985-9

[34] Q. Jiang et al., "Robust Chaotic Map-based Authentication and Key Agreement Scheme with Strong Anonymity for Telecare Medicine Information Systems," in Journal of Medical Systems 38, 12 (2014), doi: https://doi.org/10.1007/s10916-014-0012-6

3[35] X. Hao et al., "A Chaotic Map-based Authentication Scheme for Telecare Medicine Information Systems" in

Journal of Medical Systems 37, 9919 (2013), doi: https://doi.org/10.1007/s10916-012-9919-y
[36] Moon et al, “An Improvement of Robust and Efficient Biometrics Based Password Authentication Scheme for Telecare Medicine Information Systems Using Extended Chaotic Maps," in Journal of Medical Systems 40.3(2016):70, doi: 10.1007/s10916-015-0422-0.
[37] S. Roy et al., “Chaotic Map-Based Anonymous User Authentication Scheme With User Biometrics and Fuzzy Extractor for Crowdsourcing Internet of Things," in IEEE Internet of Things Journal, vol. 5, no. 4, pp. 2884-2895, Aug. 2018, doi: 10.1109/JIOT.2017.2714179.
[38] Y. Lu, L. Li, H. Pengand Y. Yang, “A secure and efficient mutualauthentication scheme for session initiation protocol,” in Peer-to-Peer Networking and Application 9, 449–459 (2016), https://doi.org/10.1007/s12083-015-0363-x
[39] Xu X, Zhu P, Wen Q , et al. "A Secure and Efficient Authentication and Key Agreement Scheme Based on ECC for Telecare Medicine Information Systems[J]," Journal of Medical Systems, 2014, 38(1):9994.
[40] K. Chain, K.-H. Chang, W. C. Kuo and J.-F. Yang, "Enhancement authenticationprotocol using zero-knowledge proofs and chaotic maps: ENHANCEMENT AUTHENTICATION PROTOCOL,"inInternational Journal of Communication System, Vol. 30, Issue 1, Jan. 10, 2018,DOI: 10.1002/dac.2945
[41] W. Liu, X. Wang and W. Peng, "Secure Remote Multi-Factor Authentication Scheme Based on Chaotic Map Zero-Knowledge Proof for Crowdsourcing Internet of Things," in IEEE Access, vol. 8, pp. 8754-8767, 2020, doi: 10.1109/ACCESS.2019.2962912.
[42] Q.Xie, W. Liu, S. Wang and L. Han,“Improvement of a Uniqueness-and-Anonymity-Preserving User Authentication Scheme for Connected Health Care,” in Journal of Medical Systems38, 91 (2014). https://doi.org/10.1007/s10916-014-0091-4
[43] L. D. Xu, W. He and S. Li, “Internet of Things in Industries: A Survey,” in *IEEE Transactions on Industrial Informatics*, vol. 10, no. 4, pp. 2233-2243, Nov. 2014, doi: 10.1109/TII.2014.2300753.
[44] C. Lee, T. H. Lin and R. X. Chang, “A secure dynamic ID based remote user authentication scheme for multi-server environment using smart cards,” in Expert Systems with Applications 38.11(2011), pp. 13863-13870, doi: 10.1016/j.eswa.2011.04.190.
[45] A. K. Das, M. Wazid, A. R. Yannam and J. J. P. C. Rodrigues and Y. Park, “Provably Secure ECC-Based Device Access Control and Key Agreement Protocol for IoT Environment,” in IEEE Access, vol. 7, pp. 55382-55397, 2019, doi: 10.1109/ACCESS.2019.2912998.
[46] Gu, H., Potkonjak, M.: Efficient and secure group key management in IoT using multistage interconnected PUF. In: Proceedings of the International Symposium on Low Power Electronics and Design (ISLPED 2018) (2018)

Maneesh Pant

Maneesh Pant is a research scholar in Uttarakhand Technical University, Dehradun. He has done his B.Tech in 2010 and M. Tech in 2015, both from CSE branch. He is currently working as an Assistant Professor in the Department of CSE, College of Engineering Roorkee, Roorkee, Uttarakhand, India. He more than 4 years of Teaching and research experience. His research areas are Internet of Things, Cryptography, Machine Learning and Cloud Computing.

Brij Mohan Singh

Brij Mohan Singh is Dean Academics & Professor in Department of CSE, COER Roorkee. He has published more than 35 research papers in International Journals such as Document Analysis and Recognition-Springer, CSI Transactions on ICT-Springer, IJIG-World Scientific, IJMECS, EURASIP Journal on Image and Video Processing etc. His research areas are Digital Image Processing and Pattern Recognition. He has guided 3 PhD Thesis of Uttarakhand Technical University (UTU) Dehradun India and currently 6 are in process.

Dharam Vir Gupta

D. V. Gupta obtained his M.Sc (Applied Mathematics) in 1982 and Ph.D. in 1991 both from University of Roorkee (presently IIT Roorkee), India. He is currently working as Professor, Dean (Basic Sciences & Humanities) & Head of Mathematics Department at College of Engineering Roorkee (COER), Uttarakhand. He has published 46 research papers in various International/National Journals/Conferences. His main research work focuses on Theory of Relativity and Queuing Theory. He has more than 32 years of teaching & research experience to his credit.

Figures

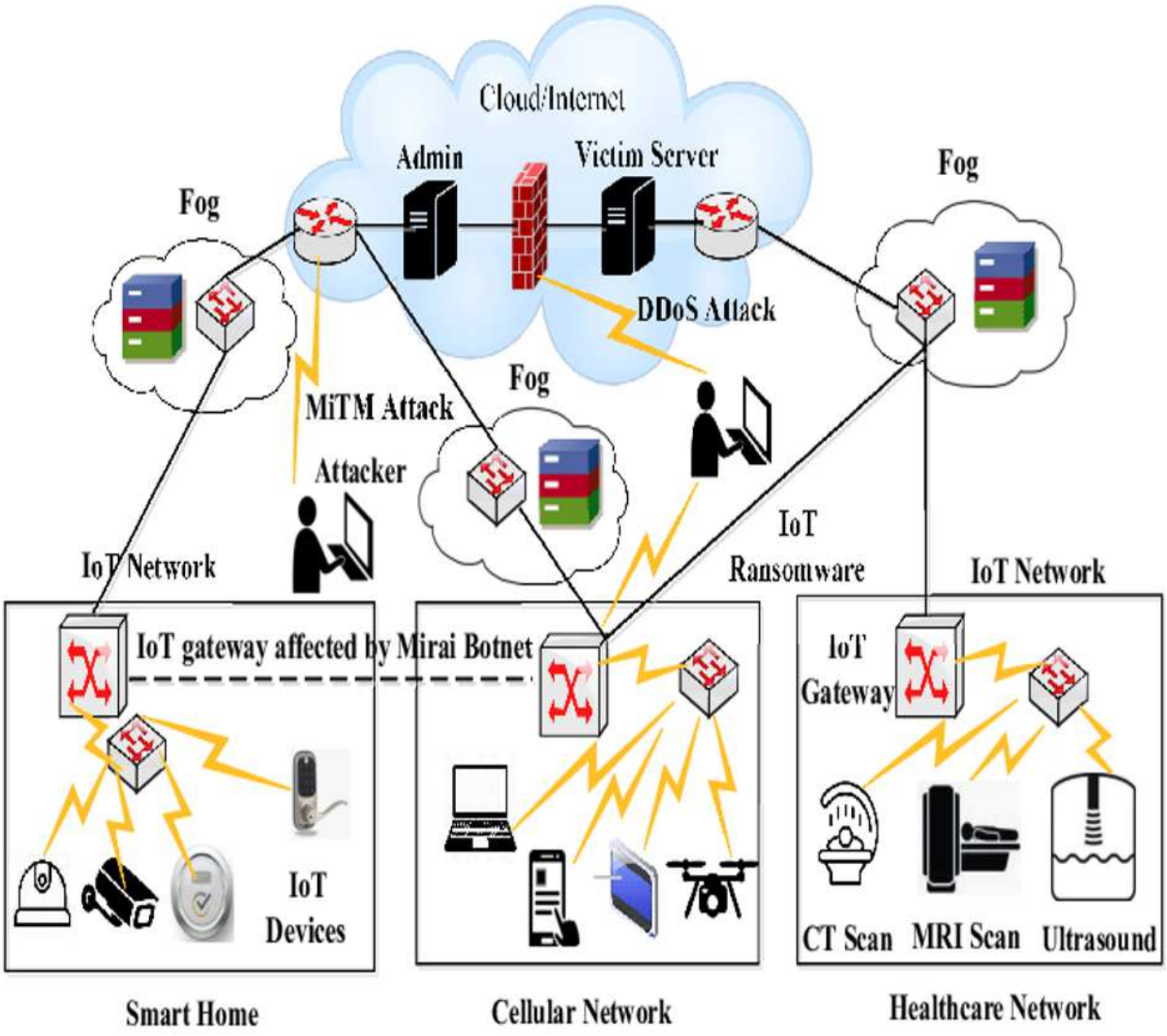

Figure 1

Shows the different IoT networks [16]

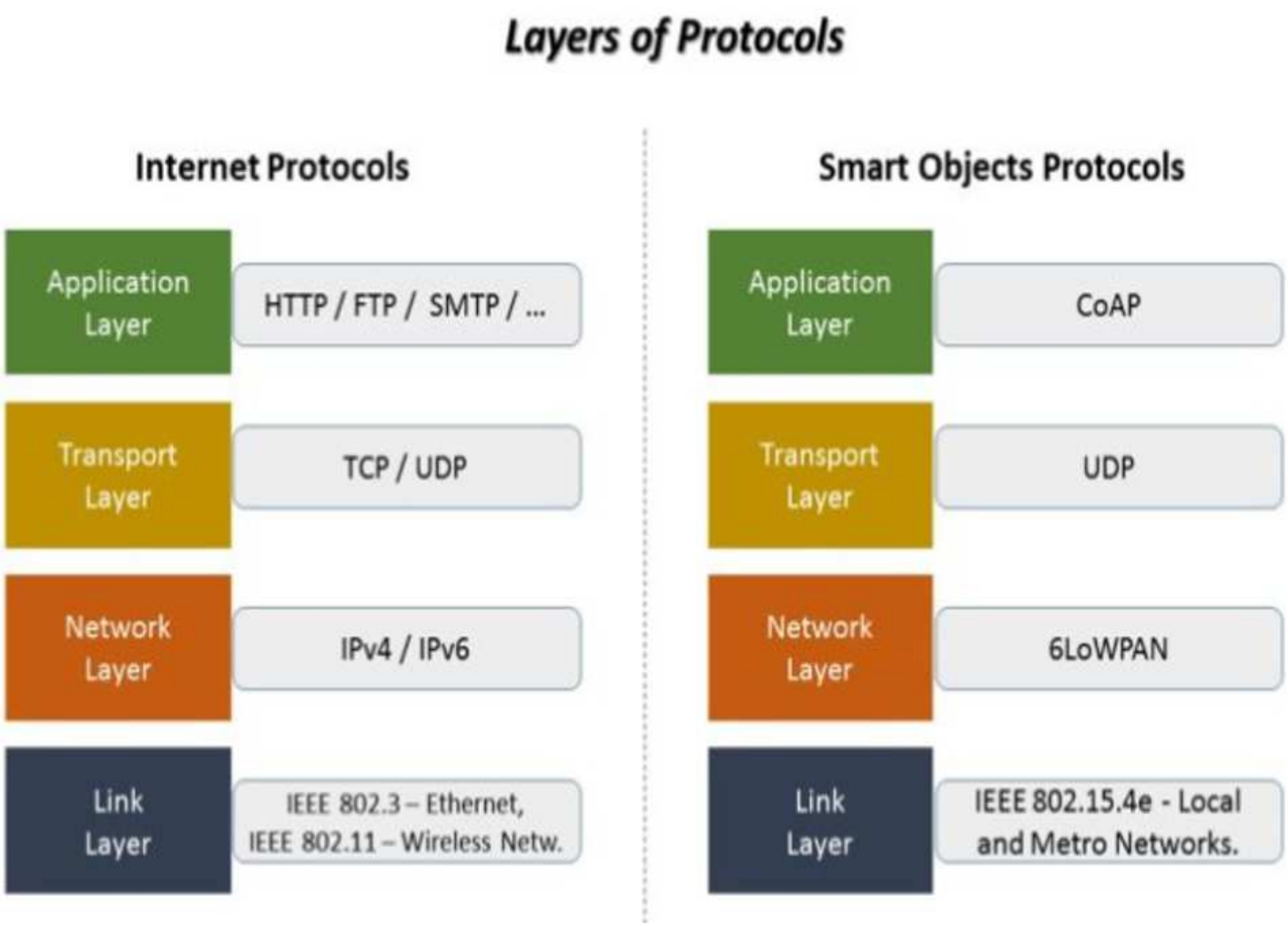

Figure 2

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

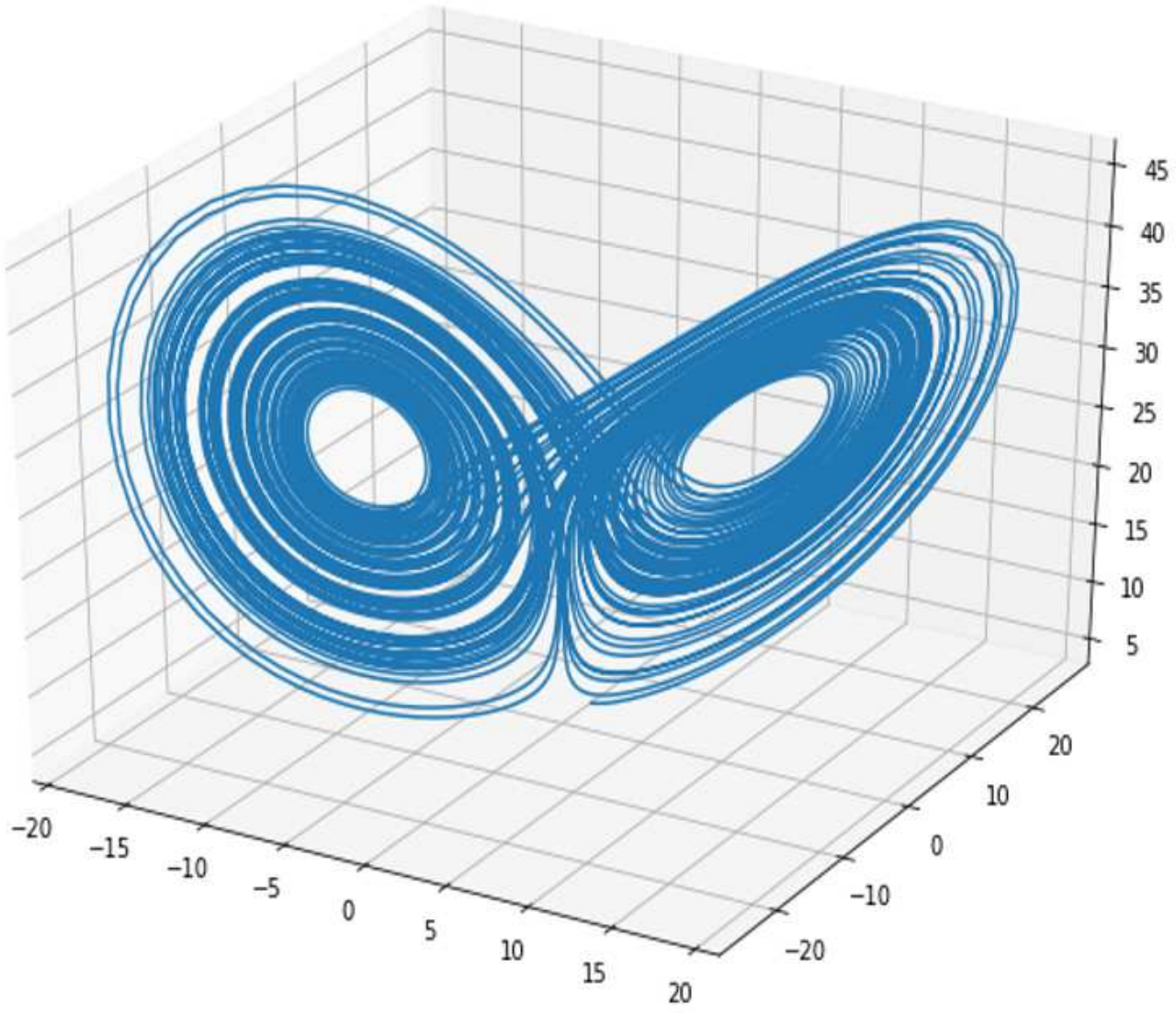

Figure 3

Lorenz map

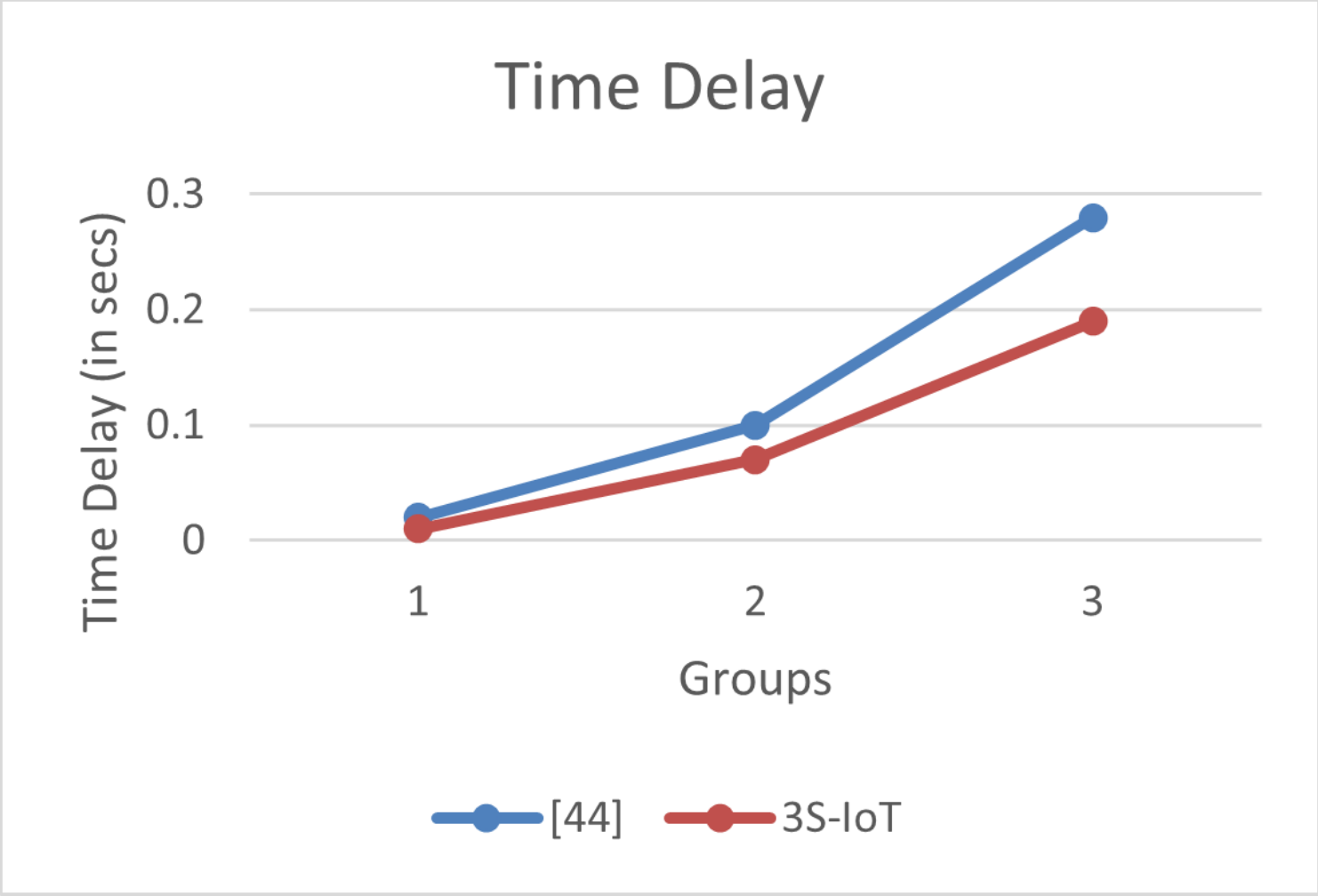

Figure 4

Time Delay

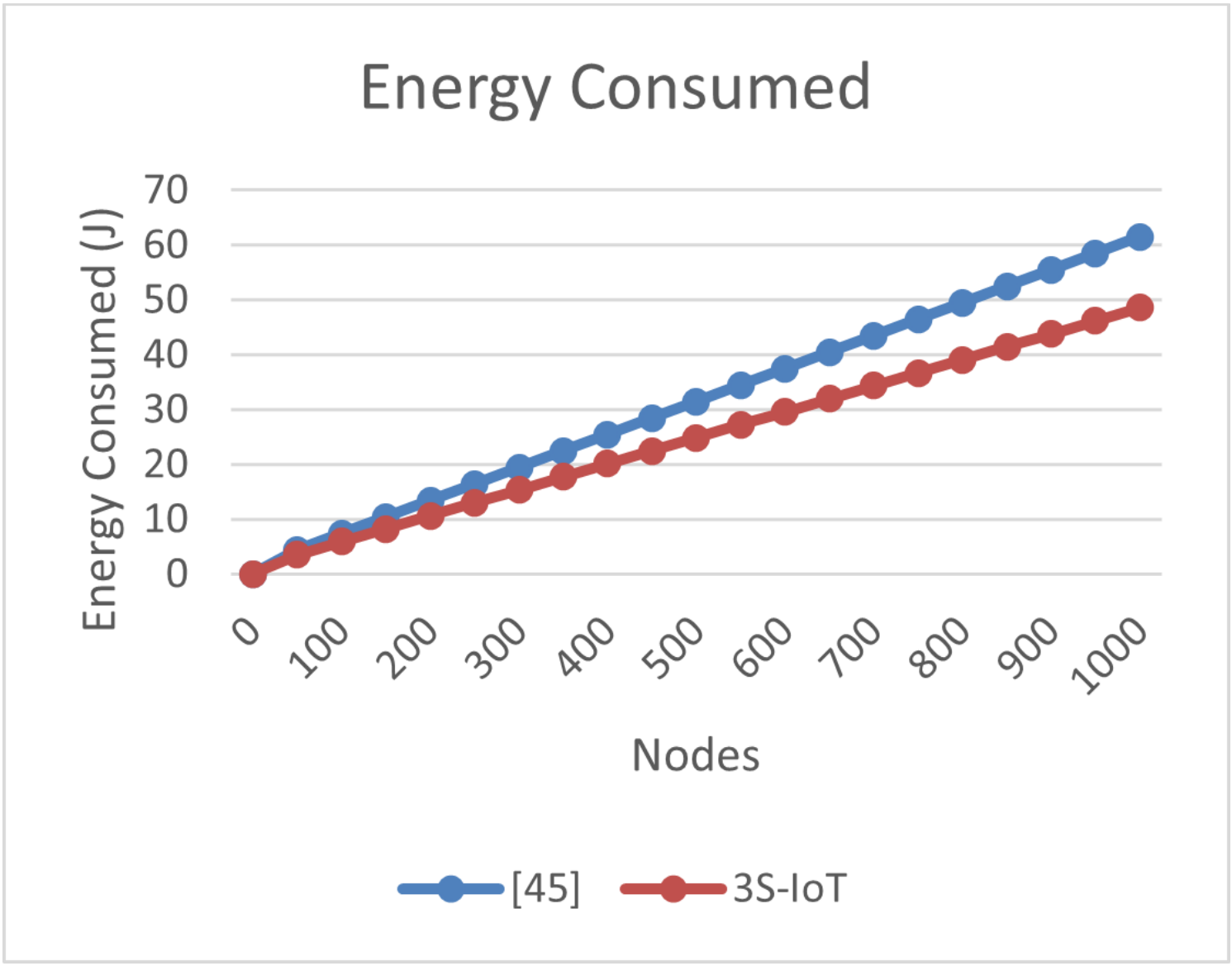

Figure 5

Energy consumed

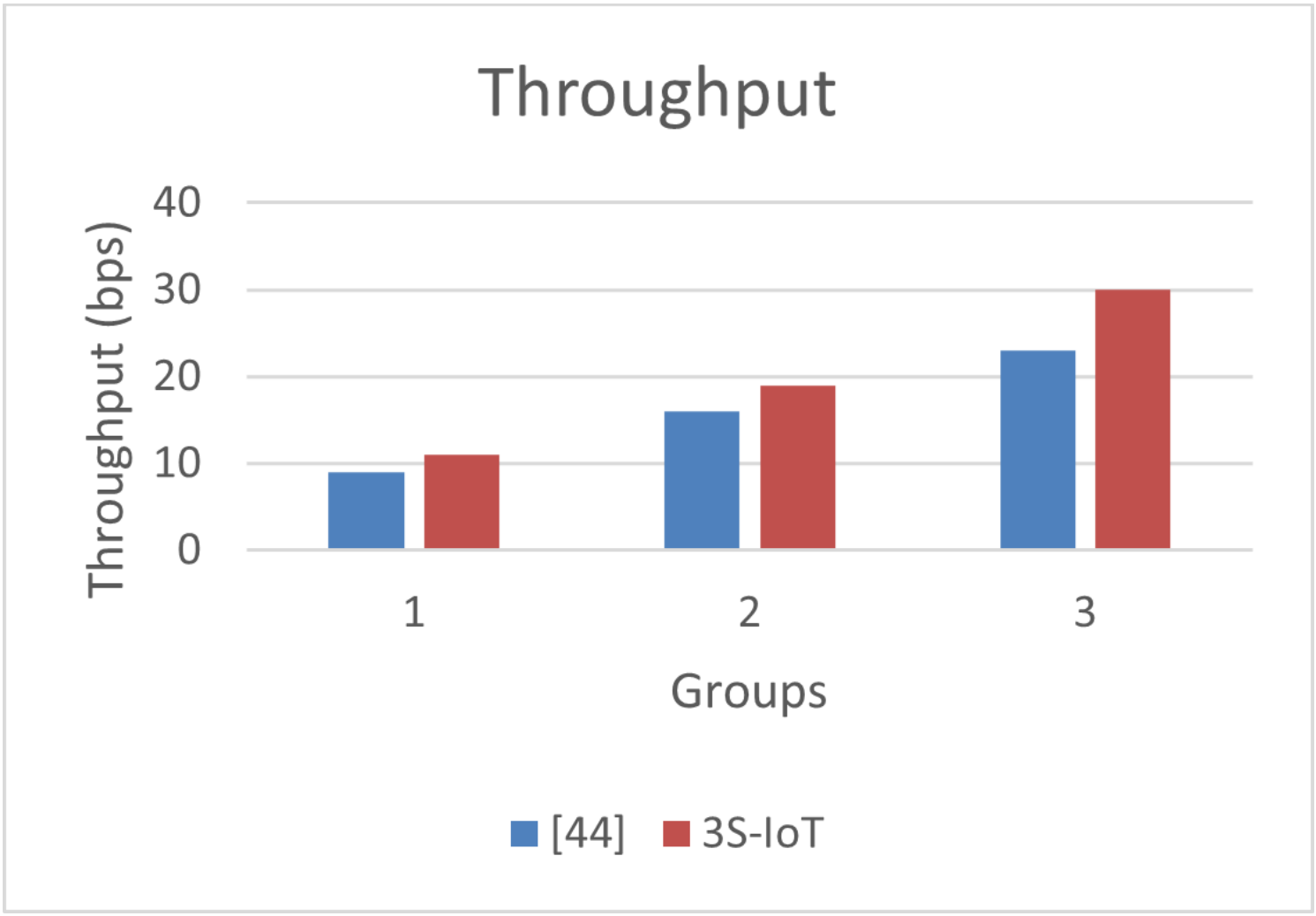

Figure 6

Throughput