Eleyon
SOUTH ASIAN JOURNAL OF
ENGINEERING AND TECHNOLOGY

Full Length Article

SECURITY FOR MULTI-HOP INTERNET OF THINGS

J.Gowthami [1], *K.Aishwariya* [2], *P.Divya* [2], *M.Kavin Kumar* [2], *A.Elangovan*[2]

[a]*Assistant professor, Department of Information Technology, Nandha College of Technology, Erode 638052 ,Tamilnadu ,India*
[b]*UG Scholar Department of Information Technology, Nandha College of Technology, Erode- 638052, Tamilnadu, India*
[b]*UG Scholar Department of Information Technology, Nandha College of Technology, Erode- 638052, Tamilnadu, India*
[b]*UG Scholar Department of Information Technology, Nandha College of Technology, Erode- 638052, Tamilnadu, India*
[b]*UG Scholar Department of Information Technology, Nandha College of Technology, Erode- 638052, Tamilnadu, India*

***Corresponding Author**
mail2gowthamij@gmail.com
(J.Gowthami)
Tel.: 9095732025

Received : 15-12-2018
Reviewed : 25-01-2018
Revised : 7-02-2018
Accepted : 02-3-2019

DOI:

ABSTRACT:Security protocols for Internet of Things (IoT) need to be light weighted due to limited resources and scalability are available in the internet. Small and low-energy devices are suitable for cryptographic solution because of their energy and space limitations. The Received Signal Strength Indicator (RSSI) is used to generate link fingerprints for communicating IoT nodes. Correlation Coefficient is used for matching the link fingerprint. Co-relation Coefficient is used to communicating secured data transfer. Adversarial Node can be detected foe specific link in between the two nodes. Data Provenance has achieved by comparison of packet header.

Keywords: Light weight, Data Provenance, Fingerprint, Adversarial Node, Received Signal Strength Indicator (RSSI)

1.Introduction

INTERNETS of Things become necessary for the future work. It controls all devices in network. More than 50 million devices will be connected through the IoT. The IoT can be connected by the following process, Medical staff. Automobile performance and statistics, Home device control, Transportation domain, Smart grids and smart meters. Data gathered from sensors and it is propagated to Internet cloud. The nodes are Large in number, Small in size, mostly accessible. At the receiving end the measures should be make that the data is secured and effectively received. IoT nodes are not physically protected therefore data security and data provenance act as backbone to implement IoT network. If any proper security. Not taken then the data can be easily forged or tempered.

The security primitives are Detection of certain attacks, Masking channel stated, Intrusion detection, Location distension and Data provenance the origin of data are find by the data provenance.[2] A single change can occur in the data that might cause big problems. Due to the energy limitations of the IoT nodes the traditional cryptographic techniques are not viable solution in IoT. For enabling end-end production it acquires, less space, Energy efficient security primitives with, less computational complexities. The IoT based network should be secured for the trust of users. The low energy requirements of security mechanism involved should be light-weighted. The authentication between the IoT nodes and the server should be secured. Accurate data provenances in the IoT node are used for improving the trust level. The data starting from the original resource that is useful for determining and describing the derivation history from the data provenance. The intellectual property and its relevance can be protected by records. The security algorithms and the cryptography techniques are used and also contain high computational complexities with high energy consumption.[1] Without using any extra hardware the light-weight security algorithm proposed for secured IoT based information exchange.By correlating the link fingerprints the adversarial node can be detected effectively in the adjacent IoT nodes. The same link fingerprints can be achieved by data provenance to find the intrusion detection in the IoT network.

II. LITERATURE REVIEW

This paper describes design approaches that blend high energy-efficient circuit techniques with optimal accelerator micro architecture data path, and hardware friendly arithmetic to achieve ultra-high energy consumption. [4]Security platforms for adoption in area/battery constrained and self-powered systems. Industry leading low energy efficiency is demonstrated. Fabricated and measured in advanced process technologies. Securing data provenance focuses only security elements on providingpartial part of in their mechanisms. Cloud not provides full protection to the data provenance as a whole Paper presents the provenance and challenges description in providing security assurances in the Cloud.

The authors of show that the received signal strength indicator (RSSI) values of a wireless channel can be used as the fingerprint of a wireless link. The RSSI values are quantized using typical quantization mechanisms such as level crossing or ranking techniques. [7]The current RSSI value of the wireless link between two parties is then used as the wire-less fingerprint for a given session. The taxonomy of attacks in IoT are spoofing, altering, replaying routing information, Sybil attack, Denial of Service attacks, attacks based on node property, attacks based on access level, attacks based on adversary location and attacks based on information damage level etc. A secured enough to gain the light-weighted trust of IoT users.

IoT network is provided using cryptographic solution to secure the Advanced Encryption Standard (AES)-128. These solutions deal with cryptography and computational complexities. That is why AES-128 algorithm is not suitable for IoT considering a large number of IoT nodes. IoT devices are secured, many research works have been conducted to counter measure those problems and find a better way to eliminate those risks, or at least minimize their effects on the user's privacy and security requirements. The survey consists of four segments. They will explore the most relevant first segment limitations of IoT devices and their solutions. The second one will present the classification of IoT attacks.

The security of different PUFs designs against these modeling attacks has been evaluated in multiple research efforts. However, a more accurate evaluation that incorporates the area fingerprints of the different PUFs is missing from the literature. Such evaluation is rather essential in order to determine the most suitable for the constrained IoT devices different PUF design. To perform this evaluation, we implemented several strong delay-based PUFs. The results that when factoring in the PUFs implementation area costs, high PUFs compare differently as some enhanced PUF designs turned out to have inferior efficiency compared to their simpler counterpart. We recognized the most effective design elements in PUFs. Based on the efficiency obtained, we recommended the optimal different security schemes used in constrained IoT devices PUF design.

III.BACKGROUND MATERIAL

The two IoT nodes are communicated between the various metric Received Signal Strength Indicator(RSSI). [5]To generate the link fingerprint, Time of arrival, Phasor information, Error vector magnitude is used. For any connected nodes there is a linear relation between the RSSI variations. It is helpful in generating the link fingerprints and it is highly correlated for two connected nodes. This information is to develop the link fingerprints. The RSSI values can be recorded in real time and its duration of RSSI values at each IoT node can be maximized or minimized depending on the power availability to the nodes. The IoT nodes are power limited and realistic

spectroscopic studies. Optical study shows that crystal is transparent in the entire visible region and discloses the suitability of the crystal for optical applications. Dielectric study shows that low value of dielectric loss at higher frequencies. [8]TG/DTA studies reveal that crystal is stable up to 90°C. Photoconductivity study ascertains the negative photoconductivity nature. Powder SHG efficiency of the grown crystal is 12 times greater than that of KDP. All the preceding results suggest that 8HQ crystal can be used as a potential candidate for photonic, electro-optic and SHG applications. approach to take the record time larger and it is not affecting the results.

In IoT network there is no adversarial node is present. [9]It is present only in between the two nodes. If the server is secured the adversarial node can send its data. The intrusion can find at last by using the data provenance. It used in real-time experiments.

1. IoTnetwork present in no adversarial node.
2. Two communicating IoTnodes present in Adversarial node.

3. Packet tempered at any IoTnode.
4. IoT node is replaced by adversarialnode.

5. Adversarialnode cansenditsdatatotheserverbutcannotaccessthedata present at theserver not secure.
6. Data using provenance algorithm

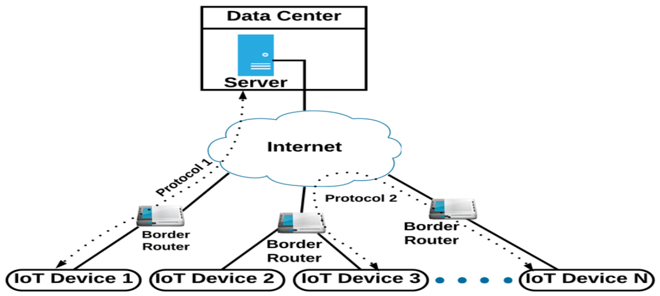


Figure1:SYSTEM MODEL

IV. MODULES

- Adversarial Node
- Data Provenance
- Link Fingerprint

A. ADVERSARIAL NODE

Each node records its RSSI values for every 20 seconds. [10]Friis transmission equation is using for calculating the signal strength

$$P_r = \frac{P_t G_t G_r}{L_p},$$

Pt –transmitted power

Pr –received power

Gt and Gr – transmitting and receiving antennas

$$L_p = \left(\frac{4\pi d}{\lambda}\right)^2,$$

d – The distance between the two communicating nodes.

The result of RSSI values are quantized by the use of word-length of 8 bits. The finite sets of values are mapped onto the amplitude values. It is divided by the Distance between minimum and maximum RSSI values.

$$\wedge = \frac{P_{r(max)} - P_{r(min)}}{L},$$

Pr (max) – maximum received power

Pr (min) – minimum received power

A value from 0 to *L*-1 is assigned for each zone of midpoint. The value of the midpoint is approximated for each sample falling in a zone. Each zone is assigned as 8 bit and it is represented as 8 bit word length of link fingerprint (LF). The link fingerprints are encoded with an 8 bit secret key for IoT node 1, IoT node 2 and also IoT node 3.

$$LF_{encoded(1\to n)} = LF_{1\to n} \square K_i.$$

LFencoded - encoded link fingerprint

In the above formula it represents logical exclusive - OR operation. *LFencoded* sends to the server and also keeps a copy with itself.[20]adversarial node can send its data to the server by replacing IoT node. The server is assumed as highly secured and the data is stored after the authentication issuccessful.

$$LF_{1\to n} = K_i \square LF_{encoded(1\to n)}.$$

The server decodes all the receivedencodedlinkfingerprintsofeachIoTnodeusing key. The server, which are assumed to be fully protected. The binary coded link fingerprints areconverted to the respective decimal values. [11]The value is between 0.8 and 1 is considered as highly correlated in a multi-hop network.

$$\rho_{XY} = \frac{cov(X, Y)}{\sigma_X \sigma_Y},$$

Cov- covariance

Σ -standard deviation

A simplified equation is,

$$-\sum \frac{\sum_{i=1}^{n}(X_i - \bar{X}) \sum_{i=1}^{n}(Y_i - \bar{Y})}{\sum_{i=1}^{n}(X_i - \bar{X})^2 \sum_{i=1}^{n}(Y_i - \bar{Y})^2}$$

The RSSI values of the packet received at communicating IoT nodes and it respective for IoT sequence of n packets. Were 1 indicates anti-correlation,0 indicates no correlation,1 indicates perfect indication.[19]Various cases are implemented and the simulation results are presented for adversarial node detection. The results are achieved by using two methods:

1)Finding Pearson correlation coefficient without using any filter.

2)Finding Pearson correlation coefficient by applying Savitzky-Golay filter.

ALGORITHM 1:Link fingerprint

```
IoT node can be initialized
RSSI value can be read from adjacent node
RSSInew[i]← RSSI[i]+gain
Quantize RSSInew[i]
Link Fingerprint[i]←Assign binary code to the Quantized RSSInew[i]
RSSIen[i] ←XOR(Linkfingerprint[i],Keynode(j))
RSSIen[i] bundled up with session identifiers
IoT node sends link fingerprint to the server
Keeps a copy of same with itself.
```

ALGORITHM 2:Adversarial node

```
Link fingerprint[i]←XOR(RSSIen[i],Keynode(a))
RSSInew[i]←binary to decimal conversion (LinkFingerprint[i])
Link fingerprint[j] ←XOR(RSSIen[j],Keynode(b))
RSSInew[j]←binary to decimal conversion (LinkFingerprint[j])
P(RSSInew[i],RSSInew[j])
if -1<p<0.9 then
return adversarial node is present
else if 0.9<p<1 then
return No adversarial node is present
else
return The RSSI values are not correctly measured
end if
```

ALGORITHM 3:Data Provenance

```
For Headeri,
    i=n→1do
LinkFingerprintHeaderi==XOR(Headeri,Keyi)
Correlate LinkfingerprintHeaderi
With link fingerprints received from IoT node[i]
if Correlation>95%then
returni←i-1
else
    Data forged between IoT node[i]and IoT node[i-1]
else if
end for
The packet of the origin is IoTnode[i]
```

B. DATA PROVENANCE

The data provenance, header information is used to reach the origin from which the data is originated. As discussed earlier, each IoT node sends the copy of the link fingerprints to the server, so all the header information will already be present at the server. [21]If the information is received at IoT node 3 from IoT node 1 via IoT node 2, the link fingerprints of header are compared at the server in sequence with copies of link fingerprints previously sent by the IoT nodes. From whichever IoT node the last header information matches, the data is originated from that IoT node. Size of header depends on the selection of packet size.

1. Link fingerprints are observed highly matched all the header data is exhausted origin. Last IoT node N from which the header data ismatched.
2. Link fingerprints showing that the data has been tempered that mismatch occurs.

The server knows the size of header that each IoT node attaches and the adjacent IoT nodes of each IoT node. In order to check the origin from which the data is originated, Server decodes the header with the keys present at the server and correlates the link fingerprint with the already present link fingerprints received from that node. If the link fingerprints match, the same process is repeated for the adjacent

IoT node(s). [12]Whilefindingtheoriginofdata,ifadversarialnodeis present between any two IoT nodes and the packet flows through adversarial node then the server will still get high correlated result by comparing the link fingerprints.

The link finger- prints will match the link fingerprints present at the server receivedfromtheIoTnode.[16]Thereasonisthatifweconsider the mentioned situation in the adversarial node is between IoT node 1 and IoT node 2, the IoT node 1 addsthe linkfingerprintattheheaderwhichisofthelinkbetweenIoT node 1 and adversarial node. Similarly, IoT node 2 adds the linkfingerprintofthelinkbetweenadversarialnodeandIoT node 2 to the packet header received from adversarial node andforwardsit.ThelastIoTnodeonreceivingit,addsitslink fingerprint. The server checks the header for the origin and gets high correlated value after decoding the header inserted byIoTnode2.As IoT nodes will be large in number, the physical protection will not be possible for most of the nodes. The data can be easily forged or tempered. If the data is tempered at IoT node 2 and sent to IoT node 3 afterwards, the data provenance cannot be achieved rather the adversarial node's involvement can be detected.

The process can tell exactly between which link the data has been forged. This is very useful information in data forensics. The highlyuncorrelated result is achieved when comparing the link fingerprints in the header and the ones present at the server. Algorithm 3 represents the achievement of dataprovenance.

C. LINK FINGERPRINT

Performed experiment show that highly correlated fingerprint are acquired.[15]After every 10 to 15 minutes, a link fingerprint of 128bit is generated by using RSSI.[17]The fingerprint and the secret key will not be shared with any other IoT nodes.High trust can be achieved using the same model in IoT environment. [13]The server assumes that the link fingerprint is encoded and decodes it with the key of that node which is replaced by adversarial node. Here after performing multiple experiments, it is observed that the correlation coefficient can be high at times but not high enoughtoremainunnoticed.

V. EXISTING SYSTEM

The numbers of nodes are large in number, small in size and mostly accessible, the measures should be taken to make sure that the data is secured and efficiently received at the receiving end. Data security and provenance act as backbone in order to implement IoT network because the IoT nodes are not physically protected easily be forged or tampered if proper security primitives are not taken. Security primitives include detection of certain attacks, masking channel state, intrusion detection, and location distinction and data provenance. Provenance is to find the origin of the data. [14]A single change in data might cause big problems e.g., in terms of medical health report generated by an IoT node sent to a doctor, meter reading sent to the company for billing according to the consumption and change in transportation system information. Therefore, thetraditional cryptographic techniques are not the viable solution in IoT because of the energy limitations of the IoT nodes.

VI. DISADVANTAGES

Primitives with less computational complexities are key building blocks for enabling end-to-end content protection, user authentication, and consumer confidentiality in the IoT world.

Less space acquiring and energy efficient security

VII. PROPOSED SYSTEM

The proposed trust model is described for cloudcomputing.Improved energy efficiency is achieved by using Gale-Shapley algorithm which matches D2D pair with cellular user equipment (UEs).Lightweight security algorithms for secured IoT-based information exchange without using extra hardware. Adversarial node is detected effectively by correlating the link fingerprints generated by the adjacent IoT nodes.The correlation coefficient is computed at the server.

Adversarial node is detected effectively by correlating the link fingerprints generated by theadjacent IoT nodes. The correlation coefficient is computed at the server. Data provenance is also achieved using thesame link fingerprints generated to find the intrusion detection in the IoT network.fingerprints are used to authenticate the integrity of data and in the detection of intrusion. Theproposed solution has less time complexity compared to other state-of-the-art available solutions.

VIII.ADVANTAGES

1) No adversarial node is present in the IoT network.
2) Adversarial node is present in between two communicating IoT nodes.
3) The packet is forged or tempered at any IoT node.
4) The IoT node is replaced by adversarial node.
5) Cannot access the data present at the server.
6) Finding the intrusion in later data using provenance Algorithm.

XI. RESULTS

EXPERIMENTAL RESULTS

The MICAz is a 2.4 GHz, IEEE 802.15.4 compliantmoteusedforenablinglow-powerwirelesssensor networks. The RSSI values are taken in real time using MICAz mote. It features a compliant radio which transceivers use in the 2400 MHz to 2483.5 MHzband,offeringbothhighspeed(250kbps)andhard ware security (AES-128). The range of the radio is 75m to 100 m outdoors and 20 m to 30 m Indoors. The MICAz MPR2400CA platform provides 4 KB of RAM, 128 KB of program flash memory and 512 KB measurement (serial) flash memory. It is very energy efficient with current draw of 8 mA in active mode and less than 15 μA in sleep mode. .The MICAz is capable of running TinyOS 2.1.2, which we use to program the MICAz motes to get the desired RSSI Values. The experiment is performed in an indoor environment. The base station and MICAz motes are shown in Fig 2a and 2b, respectively, while the layout of experimental premises.The base station is positioned at the lobby to generate log files having RSSI values in dBm of each MICAz mote.[18]Three MICAz motes move randomly in the lobby, halls and labs to generateRSSI values and send their respective RSSI values to the static base station. The MICAz motes do not cross each other.Theorientation of the MICAz motes is kept in a way as shown in Fig 1. The RSSI values are plotted in Fig 4 and 6 with a gain provided to all RSSI values received in order to make them positive.

1. DATA PROVENANCE

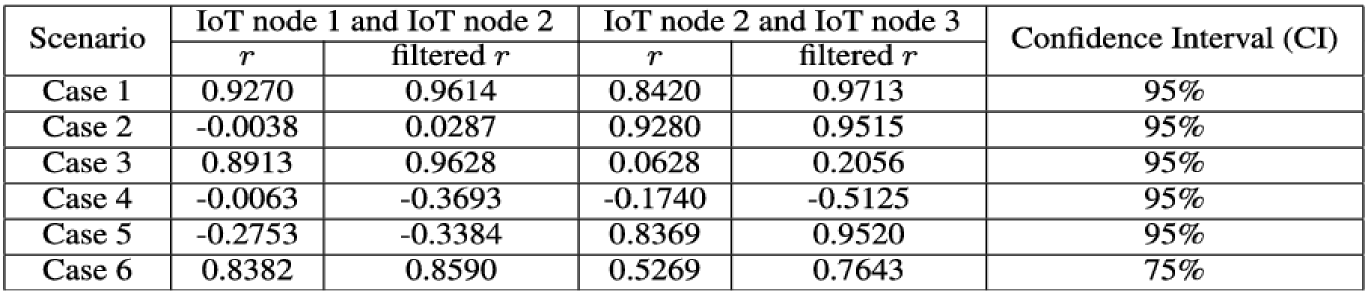
Data provenance has been achieved using the same data received at the base station as described in subsection IV-A. Simulation is performed for two cases. They are as under.

Case 1: No forging of data

Thefirstcaseiswhenthepacketistransferredfromlotnode 1 to IoT node 3 via IoT node 2, IoT node 1 attaches the encodedlinkfingerprinttotheheaderandsendsitto IoT node 2 attaches two encoded link fingerprints to the header. One of link A and other of link B as shown in Fig1.IoTnode3uponreceivingthepacketaddsitsencoded link fingerprint to the packet. When data provenance has to beperformed,thepacketheaderisdecodedinbeperformed,thepacketheaderisdecodedinsequenceatthe server.Firstly,thelastinsertedpacketisdecodedwiththekey associatedwithIoTnode3andlinkfingerprintsarecompared withalltheavailablelinkfingerprintsreceivedfromIoTnode.

Case 2: Packet is forged at the node level.

This case represents a situation when packet is forged at IoT node 1 and is received at IoT node 3 via IoT node 2. The process described in case 1 of subsection IV-B2 is applied by decoding the header in sequence with the key of that IoT node and comparing it with all the available linkfingerprints.beperformed,thepacketheader



Scenario	IoT node 1 and IoT node 2		IoT node 2 and IoT node 3		Confidence Interval (CI)
	r	filtered r	r	filtered r	
Case 1	0.9270	0.9614	0.8420	0.9713	95%
Case 2	-0.0038	0.0287	0.9280	0.9515	95%
Case 3	0.8913	0.9628	0.0628	0.2056	95%
Case 4	-0.0063	-0.3693	-0.1740	-0.5125	95%
Case 5	-0.2753	-0.3384	0.8369	0.9520	95%
Case 6	0.8382	0.8590	0.5269	0.7643	75%

TABLE 1: Pearson correlation coefficient ® calculated various case

Scenario	**Correlation of IoT node header with all available LFs at the server**				**Remarks**
Case 1	**100%**	**100%**	**100%**	**100%**	**The origin is IoT node 1**
Case 2	**100%**	**100%**	**100%**	**40.7407%**	**The data is tempered at IoT node 1**

TABLE 2:Data Provenance

2. ADVERSARIAL NODE

The results are achieved by using twomethodsLink fingerprints are observed highly matched all the header data is exhausted origin. Last IoT node N from which the header data ismatched.Link fingerprints showing that the data has been tempered that mismatch occurs.

Case1: IoTnetwork present in no adversarial nodeThe RSSI variation comparison of link A and link B respectively as shown in Fig 1. IoT node 1 communicating with IoT node 2 and IoT node 2 communicating with IoT node 3 are showing the highly correlated pattern. The correlation coefficients achieved are 0.9270and 0.8420, respectively. A higher value of 0.9614 and 0.9713 are achieved by applying the filter, which further smooth's down the RSSI variations. comparedtothelink fingerprintsofIoTnode2.Fig10representstheuncorrelated plot for both filtered RSSI variations. The correlation ishigh between the RSSI variation patterns of IoT node 2 and IoT. IoT node 2 will be different. The correlation is quite obvious in Fig 8 by observing the relationship inRSSI

Case2: Two communicating IoTnodes present inAdversarial node.As the adversarial node is present between IoT node1 and IoT node 2, the link fingerprints generated at IoT node 1.

Case3: Packet tempered at any IoTnode.

The comparison of RSSI variationsis presentedinFig9.BothIoTnode2andIoTnode3sendtheir respective encoded link fingerprints to the server.

Case4: IoT node is replaced by adversarialnodeLink fingerprints mismatch at the server because the RSSI variations comparison is uncorrelated. The reason is that they are connected to the adversarial node. The linksare establishedthroughtheadversarialnodes.Wearegettinglow correlationcoefficient

Case5: Adversarialnode cansenditsdatatotheserverbutcannotaccessthedata present at theserver not secure.In this case, IoT node1sendsadifferentlinkfingerprint.

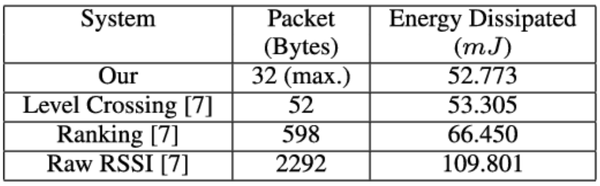
Case6: Data using provenance algorithm

The encoded data to the server. The server assumes that the link fingerprint is encoded and decodes itwith the key of that node which is replaced by adversarial node. Here after performing multiple experiments, it is observed that the correlation coefficient can be high at times.

3. LINK FINGERPRINT

The standard values specified for MICAz motes are used for energycalculations. Furthermore, the energy benchmarks of MICAz motes used intheliteratureareappliedtothepresentedprotocols.Theenergy consumption for AES-128 encryption (128 bits), SHA- 1Hash(64bits),ECDSA-160SignandTransmit1bitare$1.83\mu J$, 154 μJ, 52 μJ and 0.6 μJ respectively. As the decoding is carried out at the server, the energy calculations are not done for the server. The server is not energy limited. Two scenarios arepresented:

1. After every 5 minutes and 20 seconds, each IoT node sendsitsrespectivequantizedandencodedRSSIvalues of 16 bytes to theserver.
2. IoT nodes add certain bytes as headers to the payload which contain encoded linkfingerprints.



System	Packet (Bytes)	Energy Dissipated (mJ)
Our	32 (max.)	52.773
Level Crossing [7]	52	53.305
Ranking [7]	598	66.450
Raw RSSI [7]	2292	109.801

TABLE3: Energy dissipation

IoT Node (123)	**Energy Dissipated (mJ)**
1	**104.406**
2	**104.814**
3	**104.406**
Network	**312.626**

TABLE4: Energy dissipated each IoT node Network

XI. CONCLUSION

A light-weight solution for the security and data provenance in IoT environment in is proposed. The energy calculations show that less energy is consumed by applying link fingerprint generation protocol. The fingerprints generated between any two connected IoT nodes are highly correlated. Introducing an adversarial node gives very low correlation coefficient. It means that the detection of any adversarial node in an IoT network can be done for low power nodes. The data forensics can also be applied by looking at the header of the last received data. The origin of data is computed by extracting the header. . Time complexity of thesystem remains the same no matter how lengthy the codebecomes.

XII. REFERENCES

[1] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A survey on security and privacy issues in internet-of-things," IEEE Internet ofThings Journal, vol. 4, no. 5, pp. 1250–1258, Oct 2017.

[2] S. Satpathy, S. Mathew, V. Suresh, and R. Krishnamurthy, "Ultra-low energy security circuits for IoT applications," in IEEE 34th International Conference on Computer Design (ICCD), 2016, pp.682–685.

[3] M. N. Aman, K. C. Chua, and B. Sikdar, "Mutual authentication in IOT systems using physical unclonable functions," IEEE Internet of Things Journal, vol. 4, no. 5, pp. 1327–1340, Oct 2017.

[4] T. Idriss, H. Idriss, and M. Bayoumi, "Apuf-based paradigm for IoT security," in IEEE 3rd World Forum on Internet of Things (WF-IoT),2016, pp. 700–705.

[5] V.S. Sureshkumar, Dr.M. Vijayakumar, "DDoS Attack Detection By using Traffic Flow Analysis for Streaming Data ",International Journal on Engineering technology and Science pp:2-7, Issue 8, volume 2,2015

[6] M. I. M. Saad, K. A. Jalil, and M. Manaf, "Achieving trust in cloud computing using secure data provenance," in IEEE Conference on Open Systems (ICOS), 2014, pp.84–88.

[7] S. T. Ali, V. Sivaraman, D. Ostry, G. Tsudik, and S. Jha, "Securing first-hop data provenance for bodyworn devices using wireless link fingerprints," IEEE Transactions on Information Forensics and Security, vol. 9, no. 12, pp. 2193–2204, Dec 2014.

[8] K. Zhang, X. Liang, R. Lu and X. Shen, "Sybil attacks and their defenses in the internet of things," IEEE Internet of Things Journal, vol. 1, no. 5, pp. 372–383, Oct 2014.

[9] V.S. Sureshkumar "Extended Framework For Dynamic Resource Allocation Using Asjs Algorithm In Cloud Computing Environment" , International Journal on Engineering Technology and Sciences, pp:1-7, Issue 8, volume 1,2014

[10] Z. Bohan, W. Xu, Z. Kaili, and Z. Xueyuan, "Encryption node de- sign in internet of things based on fingerprint features and cc2530," in IEEE International Conference on Green Computing and Communications (GreenCom), Internet of Things, and IEEE Cyber, Physical and Social Computing (IoT/CPSCom), 2013, pp.1454–1457.

[11] V.S. Sureshkumar "Optimized Multicloud Multitask Scheduler for Cloud Storage and Service by Genetic Algorithm and Rank Selection Method" ,International Journal of Advanced Science Engineering and Technology , pp:2-7, Issue 4, volume 3,2014

[12] Y. Xie and D. Wang, "An item-level access control framework for inter- system security in the internet of things," vol. 548-549, Apr 2014, pp. 1430–1432.

[13] Wang, D. Chen, N. Zhang, Z. Qin and Z. Qin, "Lacs: lightweight label-based access control scheme in IoT-based 5g caching context," IEEE Access, vol. 5, pp. 4018–4027, 2017.

[14] Z. Zhou, C. Gao, C. Xu, Y. Zhang, S. Mumtaz, and J. Rodriguez, "Social big-data-based content dissemination in internet of vehicles," IEEE Transactions on Industrial Informatics, vol. 14, no. 2, pp. 768–777, Feb 2018.

[15] Z. Zhou, K. Ota, M. Dong, and C. Xu, "Energy-efficient matching for resource allocation in d2d enabled cellular networks," IEEE Transactions on Vehicular Technology, vol. 66, no. 6, pp. 5256–5268, Jun 2017.

[16] Z. Zhou, H. Yu, C. Xu, Y. Zhang, S. Mumtaz,andJ. Rodriguez, "Dependable content distribution in d2d-based cooperative vehicular networks: A big data-integrated coalition game approach," IEEE Transactions on Intelligent Transportation Systems, vol. 19, no. 3, pp. 953–964, Mar 2018.

[17] Micaz-Wireless Measurement System, Crossbow Technology, 42007.

[18] C.-L. Wu and C.-H. Hu, "Computational complexitytheoretical analyses oncryptographicalgorithmsforcomputersecurityapplication,"inIEEE

[19] J.-Y. Lee, W.-C. Lin, and Y.-H. Huang, "Alightweight authentication protocol for internet of things," in International Symposium onNext- Generation Electronics (ISNE), 2014, pp.1–2.

[20] M. N. Aman, K. C. Chua, and B. Sikdar, "Secure data provenance for the internet of things." ACM Press, 2017, pp. 11–14.

[21] V.S. Sureshkumar, A.Chandrasekar, "Fuzzy-GA Optimized Multi-Cloud Multi-Task Scheduler For Cloud Storage And Service Applications", International Journal of Scientific & Engineering Research , Volume 4, Issue3, March-2013

[22]