International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-10, August 2019

Secure and Authenticated Naming Scheme for IoT Devices in Heterogeneous Networks

Tamizh selvan. C, V. Vijayalkshmi

Abstract: ***Naming the device is the main challenge in IoT and getting authentication from the sensors is possible only with secured naming services. Naming a form of addressing the sensor nodes should be readable or understandable by humans or M2M communications. Existing naming schemes have scalability and security limitations. Hence, this paper proposes an efficient and secure distributed naming scheme for IoT in heterogeneous network. Hyper -Elliptic Curve Diffie - Hellman Key Exchange (HECDH) is used in the naming scheme for the exchange of keys. This technique reduces the communication and computation complexity. The heterogeneous model of the proposed technique is simulated and the analysis has been carried out. Digital Signature (i.e., Private Key) is used to verify the node authencity. Monitoring of the node in the network is implemented using IP based Position monitoring and Intruder Detection system (IDS) is implemented for detecting the attacks. The performance metrics such Energy consumption, PDR, Total Traffic, Delay, Average Response Time and Throughput of the proposed model was simulated using Contiki / Cooja version 2.7 simulator.***

Keywords: DIstrubed NAming Scheme (DINAS), Naming, Attacks, , HECDH, IDS

I. INTRODUCTION

IoT is a rapid developing technology in wireless communication which changes the way in which humans live. In Heterogeneous system each and every layer uses different technology which consists of various sensor devices. IoT devices are very smaller and cheaper and it is used for different sensor capabilities, metering and health care, etc. In IoT, system creates a network between the devices. IoT devices like smartphones, personal computers, home appliances and thermostat or any other device needs a naming service. IPV6 has a capability of connecting billion or trillion of IoT devices to the IoT environment because IPV6 potentially has unlimited address space when compared to IPV4.

Naming a node in the network is very much complicated and depends whether the network is homogeneous or heterogeneous. Naming system is jointly formed by Naming and locating facilities and it gives a detail of the node to the user where the node is actually present at the time. Naming services have a lot of information like
usernames, access permission, host address, password, host name etc., and all this information are stored in a server which enable consumer objects and application to be connected between the networks. The users can access the information of named objects from the naming server. This paper proposes a new naming service called Secured DIstributed Naming Service (S-DINAS) which increases the security in the naming and also protects the IoT devices from various security attacks in IoT environment. This proposed naming scheme includes

- Secured DIstributed Naming Scheme (SDINAS) naming scheme for naming and managing IoT devices efficiently.
- Implementation of SDINAS using ECC and HECC for enhanced security and comparison of their performance analysis.

Section 2, summarizes related work relevant to existing naming service. Section 3, describes the proposed naming system S-DINAS. Section 4, Performance of S-DINAS based on two security algorithms (ECC and HECC) is analyzed. The paper is concluded in section 5.

II. RELATED WORK

IoT is popularly used in various internet services. The main aim of IoT is to develop a wireless network in which each and every node have been identified by a unique identifier. It is very easy to communicate between the nodes when the naming process is enabled and secured properly. Device Discovery is used to find the neighbouring nodes and to create a routing path. In an IoT environment, each IoT device is identified by a Naming System in which the devices are from the similar manufacturer and device type.

Domain Name System (DNS) server is placed at the border router and it stores all binding information's and gives the response to all name resolution queries but DNS server requires a DNS. In DNS, the actual name to IP address mapping, enables the nodes to locate each other on an internetwork. DNS name service uses a client server mechanism for host address information. The above technique may lead to large overhead and high energy consumption and also is very difficult to configure sensors domain names in the DNS. When the number of devices increases the translation between the domain names and IPV6 addresses is done by DNS server once DNS is allowed to translate.

Michele Amoretti (2017) et al., proposed a naming approach and service discovery in WSN denoted as DINAS. In DINAS approach a new binding propagation scheme called RPL-DHT was analyzed. Performance analysis was carried out using different topologies with different sizes by hybrid simulation.

Manuscript published on 30 August 2019.
***Correspondence Author(s)
Tamizhselvan. C*, Research Scholar, Department of ECE, Pondicherry Engineering College, Puducherry, India. Email: cptamilselvan@pec.edu
Dr. V. Vijayalakshmi, Associate Professor**,** Department of ECE, Pondicherry Engineering College, Puducherry, India. Email: vvijizai@pec.edu

In DINAS, all the process is executed step by step only. A node is created by using three pillars (Bloom filters, name address bindings and Caches) and propagates all the information (name-address) about the nodes to another nodes. Destination-Oriented Directed Acyclic Graph (DODAG) is constructed by the network using RPL protocol. In DODAG each and every node transfers its name binding information to its parent node and it spreads the binding further down to a sub graph limited by levels.

In proactive manner all the nodes propagate the name binding notifications periodically between the neighbouring nodes in the network and it stores the similarities in the caches for upcoming name resolution queries. If any changes in the topology, caches and names occur, they are updated periodically. In DINAS, the main drawback is security.

Lijun Dong, (2017) et al., Proposes a name resolution method which guarantees to overcome node failures. Once the Home Node fails it transfers the records of the node to another ICN node. This model gives exact information to the server with minimum overhead and also updates the naming information. To give guarantee for accurate resolution, the Home Node will be fine-tuned with minimum delay due to server presence/absence. This naming approach gives a provision to large number of objects as well as users.

Keuntae Lee (2016) et al. proposes an efficient and confidential system for DNS name auto configuration. With Near Field Communication (NFC) devices and a Server (i.e. Authentication Server), the DNS name registration of their IoT devices can perform easily by users using Secure DNS Name Auto configuration. When the IoT devices increases, Secure DNS Name Auto configuration is a promising methodology for securing IoT DNS naming service.

Jordi Mongay Batalla. (2013) et al. The ID layer, depends on Name-Oriented Networking (NON) paradigm. The ID Layer makes no difference in the network level ID layer is built on top of it the network layer offering NON-network facilities, caching of IoT data and location or ID. This approach is used to avoid overlay and achieves more efficiency and is a simplified approach for IoT related operations implementing object/service i.e., object registration /service registration, object searching /service searching and data delivery.

Ye Tian (2012) et al. Resource Name Service (RNS) is used to provide a compact and realistic naming service in IoT. To overcome the heterogeneity problem of current identification issues, two - stage Object identification was designed. Standard Identifier (SID) and Resource Identifier (RID) are the two-stage identification used to resolve Flat structure based Distributed Hash Table (DHT) and Tree structure-based DNS. The most famous function in IoT name service is Information Location. Auxiliary authentication and anti-counterfeiting, etc., are the other functions which is provided by IoT name service based on RNS.

In section III, a Naming Service Scheme is proposed effectively for the Wireless Sensor Network with IPv6 based network.

III. PROPOSED NAMING TECHNIQUE FOR IOT NETWORK

An efficient and secure naming technique "Secured Distributed NAming Service (SDINAS)" is proposed for heterogeneous network in IoT environment. The objective of the proposed technique is to assign a name to the nodes in the networks. The Naming Scheme of the proposed work uses Hyper Elliptic Diffie Hellman key exchange method (H-ECDH) for exchange of keys and Intrusion Detection System (IDS) for detecting attacks. Security has also been improved (Hyper Elliptic Curve Cryptography) HECC algorithm. HECC is used in the SDINAS for the key exchange process to incorporate server and the client in the network. The equation for a hyper-elliptic curve (C) is given as

C: y2+ h(x) y = f(x); h; f 2 K[x]; Deg (f) = 2g + 1; deg (h) < g;

(1)

Where, f is monic and genus (g) = (deg (f)-1) =2.

By group law, "Jacobian variety of C over a field K, is a finite abelian group. Thus, a Hyper-Elliptic Curve (HEC) over Finite Field Fp" is defined as:

C: y2+ h(x) y = f(x) (mod p); h, f ϵ K[x]; Deg (f) = 2g + 1; deg (h) <g

(2)

For authentication key exchange process will be carried out to prevent the network from attackers and also to improve the security of the network. Intrusion Detection System (IDS) is proposed along with SDINAS to improve the network stability and security. IDS detect the malicious nodes in the network.

3.1. Proposed Model of S-DINAS

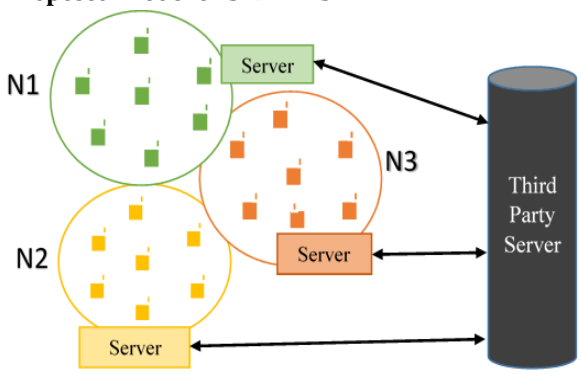


Fig.1. System Model

In Fig: 1, N1, N2, N3 are the three different network models of naming services in IoT environment. All the networks are connected with their own internal server. Sink or server is connected with the cloud or third-party server. Mostly all functions in the network are carried out by the internal server only.

To improve the network security and to store the backup of all the data, third party server or cloud is used in the network and the internal server maintain the key exchange process. When the node moves from N1 to N2, the node shares the information to the server and also finds the shortest path using DODAG. All the function of nodes is monitored using the server. In case of mobility when the nodes move from its position, the IP based position monitoring system is turned on and gives the exact location of the node continuously and updates the node location to the server. Name of the node is assigned by the internal server which is prescribed in the format of Fig. 2. Once the key exchange process is done successfully, the server assigns name to the node.

The proposed method involved with this methodology of naming is described below. Every network has a Layer ID and Unique ID. The Layer ID represents the nodes which belong to the respective network and Unique ID represents the name of the node in the network. When the nodes move starting from one network to the next network, the authentication of the nodes is given by the HECC key exchange strategy. It checks i.e., authenticates whether the node is validated or not and also confirms the node reliability. Once the node is authenticated it sends the information to the internal server to assign the node name and updates in the Third-Party Server or cloud. In case, a node is not authenticated, it then sends the message to the internal server to activate Intrusion Detection System (IDS). Proposed algorithm for SDINAS is as follows

- Step 1: Create the node and its description based on bloom filter
- Step 2: Generation of Key based on HECDH cryptography
- Step 3: Distribution of key to the mobile nodes by the sink/server
- Step 4: Propagation of messages
- Step 5: Signature of the messages with the private keys and send it to the sink node
- Step 6: Check for authentication of the node
- Step 7: If Yes, Accept the message and send it to the server to assign a name to node
- Step 8: If No, then the Intrusion Detection System (IDS) is activated and the type of attacker is analyzed. The message is rejected and the name of the node is removed from the neighborhood list

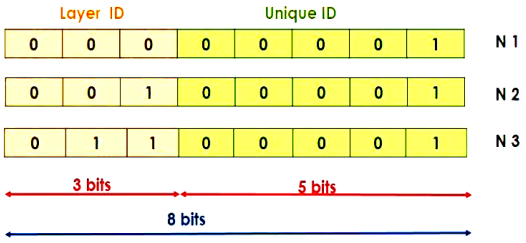


Fig 2: Naming format

Fig 2. shows the format of proposed Naming Scheme. Totally 8 bits are considered in the naming format. The first three bits denote the Layer ID and the last five bits denote the unique ID of individual network. In some cases, when the nodes in network are more than 32, naming becomes difficult. In such cases Unique ID is changed from 5 bits to 6 or 7 bits according to the number of nodes presented in the network. The layer ID of the three networks are distinctive Layer IDs. Whenever the nodes move from one layer to another (i.e. N1 to N2) the name changes according to the layer in which the node is present. Fig.3, shows the movement of node R in secured network with proposed naming service.

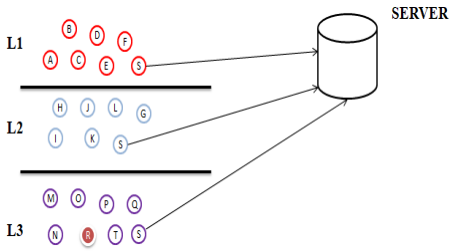
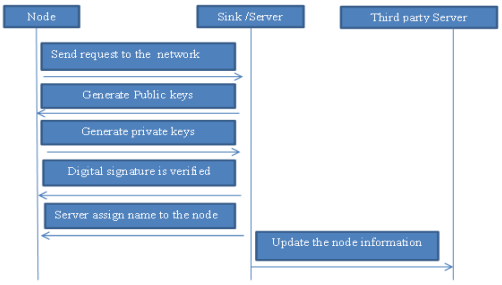
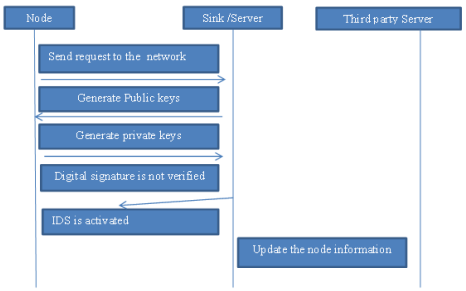


Fig 3: Suggested Network with naming service



(a)



(b)

Fig 4: (a) Flow diagram of S-DINAS (b) Flow diagram for S-DINAS with IDS

Fig 3 and 4 shows the node movement of the proposed naming Service. For Key exchange and node authentication, Hyper Elliptic Curve Diffie Hellman Key Exchange (HECDH) is implemented in IoT. Every layer has its own individual network models. Three internal server and one third party Server are deployed in the network. At the point when a node R from Layer 3 moves to the Layer 2, the Layer ID of that specific node changes to 001 from 011.

The Layer L3 server or sink begins the key exchange procedure to the L2 server or sink. The server can perform authentication process by using Hyper Elliptic Curve Cryptography and send the path to the node. By utilizing Hyper Elliptic Diffie Hellman Key Exchange, the sink 2 and sink 3 experiences the key exchange process. The public key to the nodes is shared by the internal server or sink of the respective network.

The private keys are traded between the nodes. The private key of the node is considered as a digital signature to confirm the node genuineness. Once the signature is confirmed the internal server or sink assign a name to the node and if the signature is not valid the IDS is activated for detecting the attacks. The key exchange process is done the node R from layer 3 moves to the layer 2 and stops its communication with sink 3. The layer ID and its Unique ID are changed by the layer 2 as per its format. All the process is finished by the internal server and repeat the key exchange process for all another node in the same. By this technique the network security is implemented and the attackers are easily identified in the proposed naming service. Due to various network conditions the unique ID of the nodes is also changed. If the same unique ID is presented in the other layer, then its ID changes or else the unique ID remains the same for the nodes. Unique ID to the nodes will distributes by the internal server or sink and finally all the process are updated to third Party server.

IV. Results and Discussion

The performance analysis of the proposed S-DINAS simulation is performed using Contiki/Cooja simulator Version 2.7 software. Energy consumption, Packet Delivery Ratio, Total Traffic, Delay, Throughput, Average Response Time and the Execution Time is analyzed for the proposed naming system. The parameters utilized for simulations are listed in Table I.

Table I: Simulation parameters

Parameters	***values***
Total Number of Nodes	60 Nodes
Area	500 m x 500 m
Transmission Power Range	31 dbm
Motes	Sky Mote
Transmission Range	50m
MAC Layer	IEEE802.15.4
Radio Access	CSMA
Curve with Genus	Genus 2

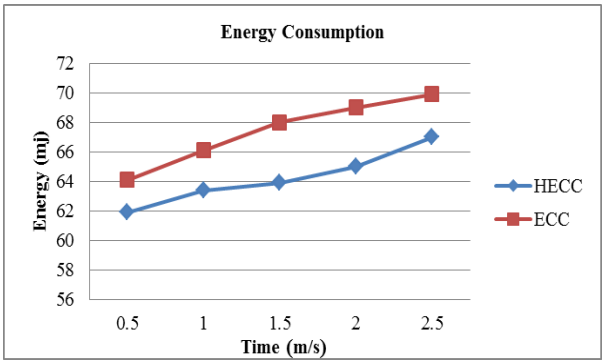


Fig 5: Energy Consumption

Fig: 5 shows the simulation for energy utilization for HECC and ECC and the obtained results were analyzed. The x-axis shows the time ms and y-axis is utilization of energy in mJ. As the simulation time increases, the energy utilization of every node increases as per time. The proposed HECC technique has lesser energy utilization of 67 mJ and ECC has an energy utilization of 69 mJ. Therefore, the proposed HECC energy consumption is 2 % lesser than that of ECC.

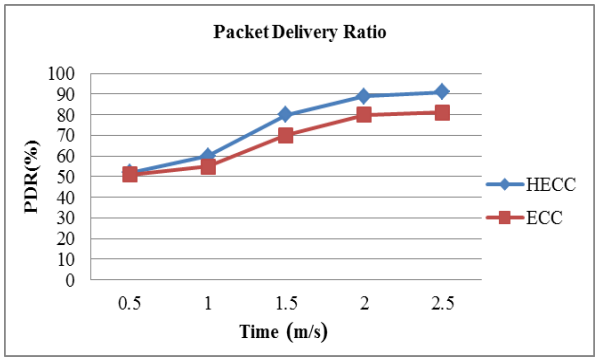


Fig.6: Packet Delivery Ratio

Fig.6. shows the Packet Delivery Ratio for both HECC and ECC. The x-axis shows the time in ms and y-axis shows the Packet Deliver Ratio in percentage. For the simulation result it can be inferred that, PDR for HECC improves by 9.4% in comparison with ECC

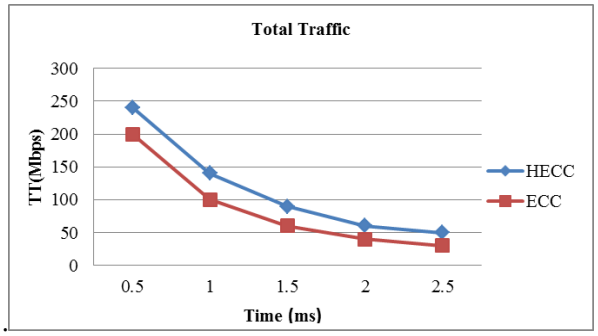


Fig 7: Total Traffic

Fig: 7 shows the simulated result of Total traffic for the HECC and ECC. The TT is initially high and continues decreasing as time increases. TT thoroughly relies upon time and information. The proposed HECC technique has a higher absolute traffic of 44ms for key sharing and name confirmation where as ECC has an all-out traffic of 23.23 mJ.

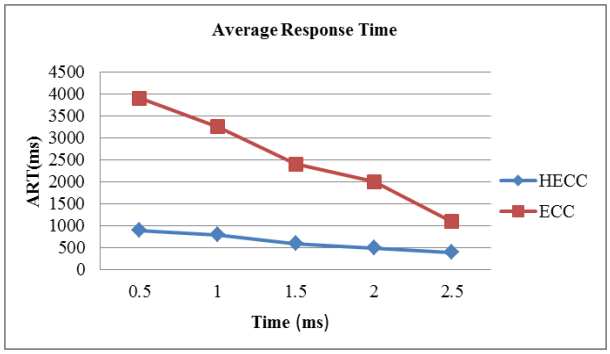


Fig: 8 Average Response Time

Fig: 8 shows the Average Response Time (ART) for both HECC and ECC. Average Response Time of the proposed system shows the time when a request is initiated and answered from the server. The proposed HECC technique has a lesser time of 340ms than that of ECC which has a response time of 1168 ms.

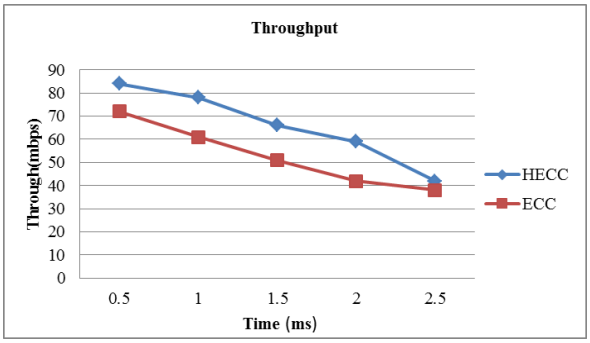


Fig: 9 Throughput

Fig: 9 shows the Throughput for both HECC and ECC. Throughput performance for ECC and HECC decreases as network load increases. with regarding time.

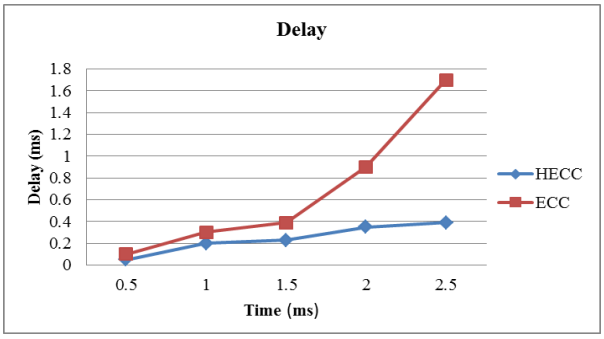


Fig 10: Comparative Delay time response of HECC &ECC

Fig: 10 Shows the delay between ECC and HECC. In comparison with ECC and HECC, has smaller key size which processing time is also low. So, delay in ECC is more when contrasted with HECC. The time for key generation for HECC and ECC shows that for ECC is 0.0984 ms and for HECC it is about 0.0535 ms. Similarly, key agreement time for ECC is 0.1601ms and for HECC is about 0.0973 ms as shown in fig 11.

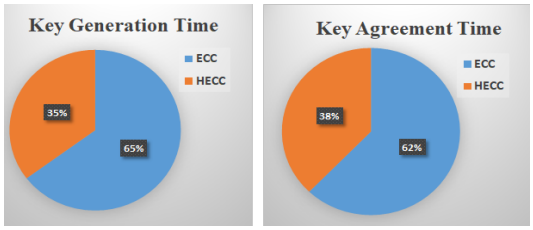


Fig 11: Comparative analysis of Key generation and Agreement time

Table II. Comparisons of performance analysis

Parameters	ECC	HECC
Energy Consumption	69 mJ	67 mJ
Packet Delivery Ratio	83.4 %	92.8 %
Total Traffic (TT)	28.23 Mbps	51.83 Mbps
Delay	1.724 ms	0.328 ms
ART	1168 ms	340 ms
Throughput	72.89 Mpbs	84.5 Mbps

Table II, shows the analysis of Energy, PDR, TT, Delay, ART and Throughput for both ECC and HECC. It is derived from the table that the HECC has better performance than ECC. The energy consumption is improved by 2mJ for HECC when contrasted with ECC. The Packet delivery Ratio of HECC is improved when compared with ECC. Therefore, in terms of all the evaluation metrics, it is inferred that the proposed SDINAS along with IDS performs well when compared with ECC.

V. CONCLUSION

In this paper a Secured DIstributed NAming Service (S-DINAS) has been proposed with HECC as a new approach in naming service for IoT, which includes a key exchange process and a naming format. The key exchange method improves the authentication of the nodes and improves the network security from the attackers. Once the node is authenticated then the server sends the information to the Third-Party Server. A new naming format was proposed for the IoT nodes which has Unique ID and Layer ID. This naming format is very useful to identify the nodes in the network and also reduces the naming problem when its scalable.

The proposed SDINAS implement for security with HECC which shows nearly 10% increase in the PDR when compared with the ECC method. Also, IDS was implemented in the proposed SDINAS which is used to detect the attackers in the network. Using this technique, the attacks are detected and removed from the network. The proposed method was simulated in the Contiki / Cooja Simulator platform and the analysis was carried out. Improved performance in terms of Energy utilization, Packet Delivery Ratio, Total Traffic, Delay, Throughput and Average Response Time was achieved.

REFERENCES

1. Michele Amoretti, Olivier Alphand, Gianluigi Ferrari, Franck Rousseau, Andrzej Duda,"DINAS: a DIstributed NAming Service for All-IP Wireless Sensor Networks," *IEEE Internet of Things Journal*, vol. 4, no. 3, pp. 1-14, 2017.
2. Lijun Dong, Guoqiang Wang, " A Robust and Lieghtweight Name Resolution Approach for IoT data in ICN", IEEE International Conference on Ubiquitous and Future Networks, pp 61-65, 2017.
3. Keuntae Lee, Hyungsuk Kang, Jaehoon (Paul) Jeong, Hyoungshick Kim, and Jung-Soo Park, "Secure DNS Name Autoconfiguration for IPv6 Internet-of-Things Devices", *International Conference on Information and Communication Technology Convergence*, pp. 564-569, 2016.
4. Kai Ryu, Yuki Koizumi and Toru Hasegawa, "Name-based Geographical Routing/Forwarding Support for Location-based IoT Services", *IEEE 24th International Conference on Network Protocols (ICNP)*, 2016.
5. Jordi Mongay Batalla, Piotr Krawiec, Mariusz Gajewski, and Konrad Sienkiewicz, "ID Layer for Internet of Things Based on Name-Oriented Networking", *Journal of Telecommunications and Information Technology*, pp. 40-48, 2013.
6. Ye Tian, Yang Liu, Zhiwei Yan, Shuangli Wu, Hongyu Li, "RNS-A Public Resource Name Service Platform for the Internet of Things", *IEEE International Conference on Green Computing and Communications, Conference on Internet of Things, and Conference on Cyber, Physical and Social Computing*, pp. 234-239, 2012.
7. K. Wang, C. Chen, W. Fang and T. Wu, "A secure authentication scheme for Internet of Things", *Pervasive and Mobile Computing*, vol. 42, pp. 15-26, 2017.
8. C. Maple, "Security and privacy in the internet of things", *Journal of Cyber Policy*, vol. 2, no. 2, pp. 155-184, 2017.
9. J. SathishKumar and D. R. Patel, "A Survey on Internet of Things: Security and Privacy Issues", *International Journal of Computer Applications*, vol. 90, no. 11, pp. 20-26, 2014.
10. S. Kumar and R. Singh, "Secure authentication approach using Diffie-Hellman key exchange algorithm for WSN", *International Journal of Communication Networks and Distributed Systems*, vol. 17, no. 2, p. 189, 2016.
11. L. Washington, "Review of Handbook of Elliptic and Hyperelliptic Curve Cryptography by H. Cohen and G. Frey", *Chapman & Hall/CRC*, 2006.
12. D. Mukhopadhyay, A. Shirwadkar, P. Gaikar and T. Agrawal, "Securing the Data in Clouds with Hyperelliptic Curve Cryptography", *IEEE International Conference on Information Technology*, 2014.
13. V. Jacobson, D. K. Smetters, J. Thornton, M. F. Plass, N. H. Briggs, and R. L. Braynard, "Networking Named Content," *ACM International Conference on emerging Networking EXperiments and Technologies (CoNEXT)*, pp. 1–12, 2009.
14. Kovacevic, J. Ansari, and P. Mahonen, "NanoSD: A Flexible Service Discovery Protocol for Dynamic and Heterogeneous Wireless Sensor Networks," *IEEE International Conference on Mobile Ad hoc and Sensor Networks (MSN)*, pp. 14–19, 2010.
15. B. Djamaa, M. Richardson, N. Aouf, and B. Walters, "Towards Efficient Distributed Service Discovery in Low-Power and Lossy Networks," *Wireless Networks*, vol. 20, no. 8, pp. 2437–2453, 2014.
16. Muneeb Ali and Zartash Afzal Uzmi ," An Energy-Efficient Node Address Naming Scheme for Wireless Sensor Networks" *Networking and Communication Conference*, pp. 25–30, Dec.2004.
17. Quazi Mamun, Muhammad Rana,"A partial key distribution protocol for WSNs in distributed IoT applications," *Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, pp. 248-254, 2017.

AUTHORS PROFILE

Tamizhselvan. C Research Scholar from Pondicherry Engineering College. He completed his B.Tech in 2009 and M.Tech in 2012 from Pondicherry University. He is having three years of teaching experience. His area of interest includes IoT, Security and Wireless Communication.

Dr. V. Vijayalakshmi, Associate Professor from Pondicherry Engineering college. She is having more than 20 years of teaching experience. Her area of Interest are Cryptography & Network security and Communication. She has published 63 international journals and 69 international conferences.