ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 3, March 2017

A Survey On Secure Connectivity Techniques For Internet Of Things Environment

[1] Mr. Vikram Neerugatti, [2] Dr. A. Rama Mohan Reddy
[1] Research Scholar, [2] Professor,

Abstract— Internet of things involves network of Nodes (sensors, Actuators, fog, cloud etc). Sensor node is a small in size, computing power and storage capacity is less. Due to this nature of Sensor the security module is not incorporated in it. So IoT Nodes has more scope for the Intruders, to attack the systems by using this weak connection of Nodes. Lot of research work has to do in this area, to establish a secure connectivity among various IoT nodes. While accomplishing the secure connectivity of things in IoT, need to consider all the security parameters like (confidentiality, authentication, integrity, etc.). The existing techniques/ Algorithms for secure connectivity of devices are not developed for nodes that which used in an IoT technology and not deal with all security parameters. This paper addressed the various existing secure connectivity techniques with advantages and disadvantages, that which is used to direct Research towards development of secure connectivity Techniques for IoT nodes.

***Keywords*— Secure Connectivity, IoT, Nodes, Smart environment, Things.**

I. INTRODUCTION

Internet of things is a large network which is inter connected with Things/ Objects that which are surrounded up in our daily life by using sensors, etc. Sensors have major capability like sensing and processing [1]. The designing of IoT network is challenging due to dynamic topology, Self organization, due to less energy, Multi node connection, etc., most of the sensors may have very low precession power etc. to coverage. They need to develop an efficient coverage algorithm with security. The major tools to provide security is cryptography by using to approach of public key and secrete key [4]. By using the automated network access elements and security elements, connectivity techniques reduce to enter the initial configuration parameter at one side. This can be achieved by "eNodeB". The "eNodeB" is a radio access network to acquire the auto connection server and initial parameters from DHCP [2].

By using traditional standards we facilitate the link layer for the mobility purpose. It has drawbacks like there is no dynamic scheme [5]. Many of IoT nodes/ Devices, Uses 6LoPAN/802.15.4, which is not good for high level of mobility without adding an extra hardware [6]. Nodes must not disturb user's daily life and may be small, need to communicate with standards protocols. This provides interoperability to extend the battery life by using low power [6].

In the context of public safety IoT nodes communication needs to be autonomous with the data can efficiently processed [7]. Internet of things uses concepts like machine to machine communication, Wireless sensor networks and technologies like RFID, cloud computing etc. It has applications in diverse areas like, Healthcare (Remotely monitoring of patience, etc.), Smart cites (Pollution, Lighting, Monitoring of systems, Smart home (Heating, Lighting), Etc. [8].

Many tradition algorithms will connect two users directly which is no true in a real world for example: Skype, Face book, Etc. where user can connect with his friends [9].

This SDN is provided to data centers, according to research survey of "Growth in data centre electricity use2005 to 2010" data centers were consumed around 1.3% of whole world electricity. It says that there power need to be concentrated, necessary to discuss some communication mechanisms, Security mechanisms for data centers [10].

The security methods can be used in device to device communications to provide security for each connection between one device to another device, in end to end connection need to provide security. The relation between each end to end connection devices, generally we use TLS and DILS techniques in the internet, which is a mathematics technique very hard to implement [11].

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 3, March 2017

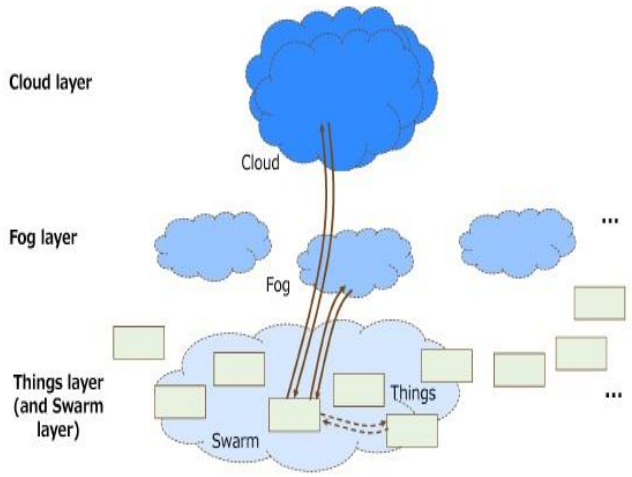

Fig 1: Layers of the internet of Things, Source: (Internet of things optical connectivity, [16])

Internet of things is a way for transforming existing static internet in to a fully dynamically future internet. Due to this more things which use in every day are connectivity to a internet which needs more security for the connectivity of IoT devices [12]. IoT is essential to concentrate on both hardware and software attacks for the connectivity. One of the attack is warm hole attack. This damages the route mechanism in a wireless sensor network. Due to this, WSN will become a anisotropic sensor network, Which leads to security threats [13].

IoNT [Internet of Nano – Things] is a new paradigm, which is use to connect in an internet, that uses to connect molecular communication for various conditions on IoNT environment. IoNT first use to define internet connection of Nano things by using individual Nano things can perform Sensing, Computing, Communication, Actuators, etc. in a network to achieve the user goals [15].

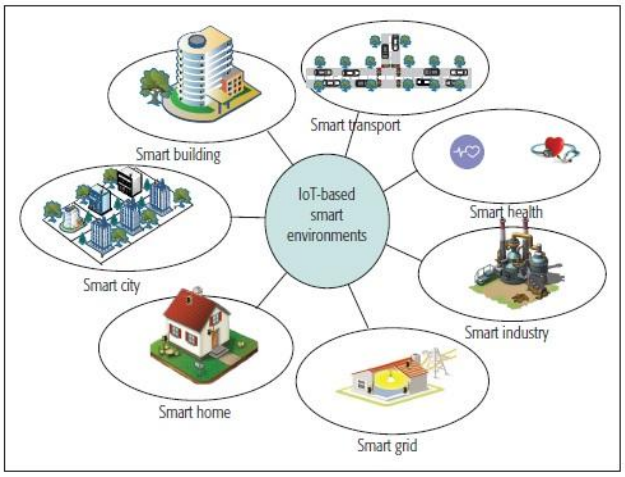

Fig 2: IoT based smart environment

Optical technology also plays a role in IoT, Which is the connectivity based technology with network intelligence etc. [16]. Rapid growth of physical things can be connected to internet with the help of sensors, Actuators, which can share information effectively, which leads to the smart environment. Several research work need to do, to integrate the IoT nodes to an internet for Smart Home, Smart Industry, etc. The various communication techniques that used in smart environment are tabulated in Table 1.

Table I Comparison of communication technologies used in smart environment [17].

Technology	Frequency	Data rate	Range	Power consumption	Application
Bluetooth	2.4 GHz	25 Mb/s	10 m	Low	Smart home
DASH7	433 MHz (Europe)	55.5 kb/s, 200 kb/s	1000 m	Low	Smart cities, smart building, smart home, smart transport, smart health
ZigBee	2.4 GHz, 915 MHz, 868 MHz	250 kb/s	Up to 100 m	Low	Smart homes, smart health
WiFi	2.4 GHz, 5 GHz	54 Mb/s, 6.75 Gb/s	140 m, 100 m	Medium	Smart cities, smart home, smart building, smart transport, smart industry, smart grid
3G	850 MHz	24.8 Mb/s	1–5 mi	High	Smart cities, smart transport, smart industry, smart grid
4G	700 MHz, 750 MHz, 800 MHz, 1900 MHz, 2500 MHz	800 Mb/s	1–6 mi	High	Smart cities, smart transport, smart industry, smart grid

The next section in this paper is organized as, in section [II] discussed about literature survey on various secure techniques for IoT, in section [III] concluded the paper and discussed on future scope.

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 3, March 2017

II. LITERATURE SURVEY

In paper [4] presents a detail approach that which is used to provide secure network connectivity called single randomly selected key. In this approach we need to randomly distribute the many encryption keys. Then need to discover the required nodes to assign the distributed keys. Once the node key identified and keys allocation to it is done, the sensor communication is established among those nodes by using symmetric encryption. The simulation is carried out in NS2 stimulator to obtain the results. The result shows that the presented approach is good to compare to existing Diffie – Hellman key exchange algorithm.

In this paper [2] presents auto connectivity for the network by providing security with network elements approach by maintaining the mutual understanding, maintenance, Operation, Administration server and network elements. In this approach we need to initially setup on IP configuration for basic connectivity. Then mutual understanding with auto connectivity server can be establish a sensor communication, after completing the auto connection server setup to identify the site and we register the hard work id, Finally we establish a secure connection with algorithm manager.

In [4] secure coverage algorithm is proposed by using virtual source algorithm [Improved genetic algorithm]. In this algorithm initially it takes the sensor location, number of generations, Population size, Mutation and recombination, Probability as input. The output generates the best sensor location. The stimulation was done in MATLAB 7.0 and provides that virtual force algorithm is best in terms of secure connectivity in coverage network.

The objective of [5] is to allow services and entities to use a nodes in an IoT with an automatically and dynamically by using symmetric procedures etc. The work proposed in this paper is an independence media approach. By using media independence techniques and with enhancements of IEEE 802.2 standards show that it has good performance in terms of connectivity. The proposed frame work is explained with scenarios like distance situations earthquake.

In this paper [6] proposed an architecture for an IoT, architecture consists of some nodes uses the (SOA) and protocols. Which increase more mobility and experiments was performed and tests proved that architecture is executing solution to achieve high performance in sensors and actuators environments.

In paper [7] discusses about the public safety problem in terms of connectivity and security. By using device to device communication approach and user equipment based connectivity, which allows a direct communication between nodes, the security is provided by using the sharing encryption keys.

Jorge Granjal et al, performed Survey analysis on existing mechanism and protocols for secure communication in IoT and present some open research challenges. For future research in this area discussed the protocol tags and various protocols like IEEE 802.15.4, IEEE 802.15.4e, 6LoWPAN, Ipv6, ROLLRPL, CoRE COAP, etc. And discussed the security requirements for communications like integrating, Authentication, Non reputation, etc. Discussed the various security nodes of IEEE 802.15.4 standards and discussed how to provide security for each and every layer of an IoT protocols. Finally discusses the open research challenges for secure communication in IoT. [8].

In this paper [9] presents a group key agreement for a local connectivity, were the user can know his neighbors by using the connectivity approach. Here individual users can initially communicate independently by using their own key allotted by centralized controller. This technique is very useful for network applications. Compare to analysis of existing traditional protocol and proposed protocol is presented with connectivity graph and proved that security is efficient way. The efficiency of proposed algorithm proved in communication cost, Communication complexity and round complexity.

This paper [10] presents a software define network based middle ware security frame work to provide security for define data centers. Software define network is a major issue is a new paradigm for an IoT, need to do lot of research work. The management and services layer architecture SDN was show in fig 3 [1].

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 3, March 2017

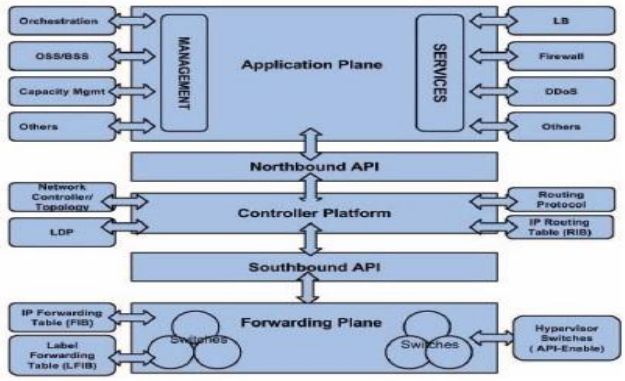

Fig 3: Management and service architecture of SDN (Source: Middleware security frame work for next generation data centers connectivity)

This paper [11] presents importance of an Iot, different IoT applications, connectivity on IoT nodes by using different standards about the components in protocols stack, some issues like security and privacy, Etc. This paper presents [12] a time reversal approaches by using digital signal processing which provide heterogeneous connectivity in IoT nodes, presented a difference between existing and proposed existing Time Reverse approach technique by using the simulations shows better performance.

This paper [13] presents a detection method for a household attacks in a node connectivity of detecting it optimizers the outing. The field theoretic analysis was discussed with the help of simulation. The proposal method was verified and approved as good methods in terms of localization accuracy.

This paper [14] presents a model of defect the failures and repairs it. And discussed about the system, Performance, Availability models and presents the illustration for the proposed models and the results proved that high performance in terms of failures and repairs for LTE technology.

This paper [15] studies the important Nano things, how it plays a role in IoT different related works on IoNT same Mattel simulations and the results and discussions in terms of the connectivity of a network.

This paper [16] discussed various optical technologies. That plays a role in IoT network users on optimal networks band width, Networking intelligence, Image sensing, Etc. and discussed some layers in IoT, Finally discussed about optical technology in IoT and various IoT applications than the users optimal technology.

This paper [17] studies an IoT based smart applications, the taxonomy of environment and the open research challenges. The taxonomy of IoT is showed in fig 4. The different entities like communication enablers, network types, Technologies, LAN standards, objectives, characteristics is clearly mentioned in the taxonomy in IoT. Discuss smart environment like smart industries, etc. Discuss some open challenges like security & privacy, Procession, Investment, Compression, Etc. In this paper discussed the benefits, Architecture, Drawbacks, Design and current going work of HIP(Host identity protocal) and discuss some problems like with solutions like “lose of universal connectivity, Support for multi- hosting and mobility, Multi cast problem and lack of privacy, Authentication, Accountability and traffic and discussed about format of control packet for HIP, Etc.

In this paper [18] present a model called dual connectivity to ensure the security for long time evaluation (LTE). In this model two evolve node B is used one of the node is to maintain and other to control the management of radio resources which is called as master ELVB and the secondary nodes, due to control other “e Node B”. This nodes model needs to secure connectivity among the nodes based upon the trust.

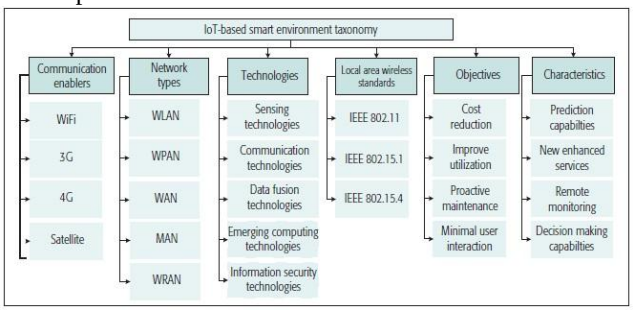

Fig 4: IoT- based Smart Environments Taxonomy Source: Internet of things- Based Smart environment: State of the art, Taxonomy and open challenges [17].

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 3, March 2017

S.NO	Techniques	Description	Advantages	Disadvantages
1.	"Single Per-Node Random Key"	In this technique, for each node in a network only single randomly selected key is assigned for establishing secure communication among the nodes in network.	It reduces the storage of different keys of symmetric algorithms and very simple.	First needs to identify the nodes to establish a network and then we need provide a symmetric encryption keys and need to distribute many symmetric keys. Takes more time.
2.	"Auto Connectivity Scheme with Security".	The network elements to accessing the network can be automatically (manual intervention is avoided) secured by using this approach.	Automatically security was provided for network elements to access the network.	Need to be a mutual authentication between administration, Operation, Maintain systems and network elements.
3.	"Multi – channel queuing models."	This is used for real scenarios in a daily life failures and there pairs was considered to know the effects of repair and failure behavior.	Both failures and repairs can be done.	Need to concentrate on both failures of channel and the performance of LTE systems.
4.	"Improved Genetic Algorithm (Virtual Force Algorithm)".	This paper proposed on secure coverage algorithm for surveillance with help of improved genetic algorithm	Maximum Field coverage for sensors.	To determine the virtual motion and then sensor parts used a repulsive force.
5.	"Media independence frame work".	This technique is used for interfacing sensors, Actuators, etc. and provides the necessary services to the users.	We can retrieve the interface and can control different entities to establish dynamic and universal connectivity.	Need to know the details of interfacing devices.
6.	"Service oriented architecture with communication protocol".	Here exchange the actuators and sensors data with an internet cloud and local cloud.	Support true mobility of IoT nodes	It concentrated only on high mobility and does not discuss on other factors in terms of performance.
7.	"User equipment based device to device connectivity".	Based upon the user experiments directly connected to the nodes without using a valuing node. Which send the data in form of broad casting nodes and provide security by using sharing exception technique.	Secure connectivity between IoT nodes	Overhead is increased by security parameters.
8.	"Group key agreement".	By sharing a secrete key called as session key among two or more parties can communicate each other.	No centralized controller of user.	The connectivity is limited.
9.	"Middleware security frame work for SDN".	It provides security based on the loading process to reduce complexity and secure connection for data contents.	Reduces complexity and establish secure connection for data centre.	All security requirements are not fulfilled.
10.	"Time diverse approach".	This use to present a heterogeneous band width at the same time. It maintains time diverse side.	No middleware and more energy efficiency.	Increasing the complexity due to the more digital processing.
11.	"Connected relation of connectivity nodes".	Proposed an algorithm that which detects the warm whole attacks. In a wireless sensor network.	No need hardware support It improves the accuracy of localization.	Time consuming process need to check the distance between the nodes and hope.

III. CONCLUSION AND FUTURE WORK

Due to rapid growth of IoT, many of Things from various discipline are connecting to an internet .To connect trillions of things to internet needs to develop on connectivity techniques with security in IoT. The existing connectivity techniques are not designed for an IoT. It is necessary for the IoT researches to develop secure connectivity techniques for an IoT.

In this paper, various connectivity techniques with security is discussed to connect different physical things which are surrounded by us in daily life to an internet. Different smart environment like (Smart city, Smart industry) communication technologies, Taxonomy was discussed. In future work, we develop the different secure connectivity algorithms to ease the connectivity between various nodes in IoT. (For example Things – Router, Router – Internet, Internet – fog, Fog – cloud, etc.).

REFERENCES

[1] Jason Barbour, Mohamed Younis, "Sensor Network Connectivity and Security Analysis Using a Single Per-node Random Key" in IEEE 2007.

[2] Henning Sanneck, ChristophSchmelz,"Auto – Connectivity and security setup for access network elements" in IEEE 2009.

[3] PekkaNikander, Andrei Gurtov, and Thomas R. Henderson, "Host Identity Protocol (HIP): Connectivity, Mobility, Multi – Homing, Security, and Privacy over IPv4 and IPv6 Networks" in IEEE 2010.

[4] JiaJie, Zhang Zhaoyang, Chen Jian, Zhao Linliang, Wang Xingwei."Integrated Coverage Control and Security Connectivity in Mobile Sensor Networks" in IEEE 2010.

[5] Daniel Corujo, Marcelo Lebre, Diogo Gomes, Rui L. Aguiar. "A Framework for the Connectivity of an Internet of Things " in IEEE 2011.

[6] Pablo Pu˜nal Pereira, Jens Eliasson, Rumen Kyusakov,"Enabling Cloud-connectivity for Mobile Internet of Things Applications" in IEEE 2012.

[7] Leonardo Goratti, ♭Gary Steri, †Karina M. Gomez and ♭GianmarcoBaldini, "Connectivity and Security in a D2D CommunicationProtocals for public safety application" in IEEE 2014.

[8] Jorge Granjal, EdmundoMonteiro, and Jorge Sá Silva, "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues" in IEEE 2015.

[9] Shaoquan Jiang, "Group Key Agreement with Local Connectivity" in IEEE 2015.

[10] Samar RazaTalpur, SamehAbdalla, TaharKechadi, "Towards Middleware Security Framework for Next Generation Data Centers Connectivity" in 2015.

[11] Joseph Decuir, " The story of the internet of things " in IEEE 2015.

[12] Yi Han,Yan Chen,Beibei Wang, K. J. Ray Liu," Enabling Heterogeneous Connectivity in Internet of Things: A Time –Reversal approach" in IEEE2016.

[13] Jiu-huZheng, Huan-yanQian, Lie Wang, "Defense Technology of Wormhole Attacks Based on Node Connectivity" in IEEE 2015.

[14] YonalKirsal∗, YoneyKirsal Ever †, "Analytical Modelling and Performability Evaluation OF LTE as dominant connectivity technology for internet of things " in 2016.

[15] Prachi Raut1, Nisha Sarwade2," Study of Environmental Effects on the Connectivity of Molecular Communication Based Internet of Nano things" in IEEE 2016.

[16] Philip N. Ji and Ting Wang, "Internet of Things with Optical Connectivity, Networking, and Beyond" in IEEE 2015.

[17] Ejaz Ahmed, IbrarYaqoob, Abdullah Gani, Muhammad Imran, and Mohsen Guizani, "Internet-of-Things-Based Smart Environments: State of the Art,Taxonomy, and Open challenges" in IEEE2015.

[18] Noomene Ben Henda, Karl Norrman and Katharina Pfeffer∗, "Formal Verification of the Security for Dual Connectivity in LTE" in IEEE 2015.