International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2015): 6.391

Study of Secure Fault Tolerant Routing Protocol for IoT

Chaithra .S[1], Gowrishankar S[2]

Department of Computer Science and Engineering,
Dr. Ambedkar Institute of Technology,
Bengaluru-560056, Karnataka, India
chaithra89raj[at]gmail.com
gowrishankarnath[at]acm.org

Abstract: ***IoT enables ubiquitous communication with different devices in a wireless network. Providing integrity, confidentiality and availability of services to access and authorization are the main challenges in IoT. For a successful communication process the path has to be established even in the presence of faults. In order to facilitate these issues the solution has to be proposed for data security assessment and penetration. In this paper RPL is used to achieve secure fault tolerant routing to enhance the performance and minimize the energy consumption. The Dijkstra's algorithm is adopted to select the paths with low cost and to store the routing information. The proposed architecture includes a Blowfish algorithm method for secure data transmission. The performance analysis of RPL is done on the basis of Packet delivery ratio and energy consumption.***

Keywords: IoT, Dijkstra"s Algorithm, RPL, Blowfish Algorithm.

1. Introduction

The Internet of Things which refers to the use of intelligent connected devices and systems for data gathered by various sensors and actuators in physical objects. The essential technologies of IoT allows anyone to connect to Internet anywhere, anyplace at anytime [1]. The „things" or objects in an IoT- such as RFID, NFS, sensors, mobile phones which uses the unique addressing scheme to interact with each other in a wireless network. The IoT devices are characterized by various features which manages the IoT devices for easyconnect environment [2].

An IoT is considered to be accessible and self-incorporating internetwork. These sorts of internetworks are profoundly inclined to [3] security and faults dangers. If these faults are not taken care of legitimately, might prompt genuine system downtime. The result of such blames would lead to the suggestions when the system utilization is basic. If there should be an occurrence of IOTs, because of their huge scale, these flaws have amplified consequences. To make IOT strong, authentic and scalable, it is important to choose a system to keep away from and encounter these shortcomings.

Due to asymmetric nature of communication between sensor nodes in IoT, security and privacy is become severe challenges. Most of the existing protocols deals with RFID suffer from threats and vulnerabilities such as insecurity, fault tolerant, inefficient identification, throughput and inadaptability. The development of RFID security protocol makes the IoT more robust distributed structure. To make IoT a robust, it is indispensable to adapt a method to avoid and counter these faults [3]. Achieving fault tolerance in IoT requires the efforts to make objects secure by default, to know the condition of the network and its services that the objects should handle the failures and attacks [4].

In this paper, an efficient fault tolerant mechanism has been proposed in addition to finding minimal path and achieving message authentication. The concept of [3] has been enhanced using the above concepts. The fault tolerance is achieved by computing the alternate path using RPL. In addition to that, the paper also aims at integrity using Blowfish algorithm and the packets are routed by finding the minimal path using Dijkstra"s algorithm.

In this paper, the section 2 illustrates the Related Work based on RPL protocols for loT platform. The section 3 elucidates various models of Proposed System. Section 4 describes the Proposed Architecture Instance used for security in IoT. Section 5 presents the performance with Results. Conclusion and References are presented in the last section.

2. Related Work

The recent trends in IoT application and WSNs can be found in [6],[7],[8] have been proposed the various aspects of security. The IoT ensures the security of all the layers. Qi Jing et al., analyzes the security issues of IoT and compares with traditional network [9]. The trusted system architecture on IoT is proposed [10] based on the research for trusted computing and trustworthy network. A systematic approach for security and threat taxonomy for IoT is proposed by [11], [12]. Solving the data security problem the trusted authentication scheme was proposed in [13] to improve the performance.

The tri-mode PKC coprocessors are implemented to support for sensed data transmission in IoT systems [24]. The various security solutions are provided for IoT includes security architecture and cryptographic mechanisms. In [25], the CSND provides the secured multi-hop routing for scalable IoT communications. The deployment of IoT raises security issues, the lightweight cryptographic algorithms are proposed for secure data aggregation [26]. The paper [27] is designed

to separate the processing and forwarding mechanisms to satisfy arbitrary objectives (energy, latency) in which CAOF allows RPL to take the sensor node with limited resources into the routing decision.

WSN is an interconnection of numerous sensor nodes with limited energy [14] which forwards the data to the destination where fault tolerant of optimal determines to enhance the network lifetime by energy balancing for forwarding data. Providing a security in RPL for various challenges where devices are connected to the untrusted Internet and resources constraints by various routing attacks. The Learning automata and cross layer design techniques are used for successful delivery of packets with faults [3] where iCLAFTRA uses diversified paths for forward data between a pair of communicating devices even in the presence of faults. The various faults tolerant issues are solved by using different methods in [3],[16], [8]. The paper [28] proposed the taxonomy to classify faults and recovery mechanisms in a network. Routing paths are computed in [29] for minimum transmission count by using TXPFI for successful delivery of data in the presence of malicious node.

Most of the existing protocols are failed or operates with low throughput for asymmetric links some people uses protocol specific approaches. To improve the fault tolerance of each node and to provide energy efficiency [17] proposed a fault tolerant multipath routing scheme (FTMRS). The [15], [18] provides the various impact of routing attacks, where as the Hao Zhang et al., proposes a security protocol in the P2P networks based on IoT and enables the connection between different protocols and devices.

For various applications, the unreliable behavior of wireless links and individual path routing mechanisms affects the performance while transmitting data from sensor nodes. A multipath solutions for RPL routing protocol [20] to achieve network load balancing, energy efficiency and delay. The Leila Ben Saad et al., proposed two case studies for the extent the lifetime of WSNs by evaluating the value of mobile nodes and another for the performances of the simulation results are compared [21].

In [30], describes the protocol attributes for unreliability issues in data delivery to provide simple routing optimization. For LLN based network the multipath routing [31] is used to achieve multifold objectives which includes fault tolerance, reliability and throughput. To support high data rates when compared to single path by forwarding node.

To improve the multiple sinks in WSN, the RPL-based protocols are demonstrated to increase in packet delivery ratio and to decrease the number of retransmission by considering the shortest hop-count metrics [32]. For the security aspects of RPL, the ETX metrics are used to analyze the vulnerability of RPL to find the routing choices (RC) intrusion to satisfy the energy efficient requirements [33]. The paper [34], focuses on possible attacks in RPL and 6LoWPAN network to which is connected to limited resources, unsecured network, lossy links.

3. Proposed System

The proposed system aims at two things:

A. **Data transmission with fault tolerance with RPL**: The RPL routing protocol is used to transmit a data even in the presence of faults. The minimal path can be determined using Dijkstra"s to transmitting a data from Base Station to its destination.

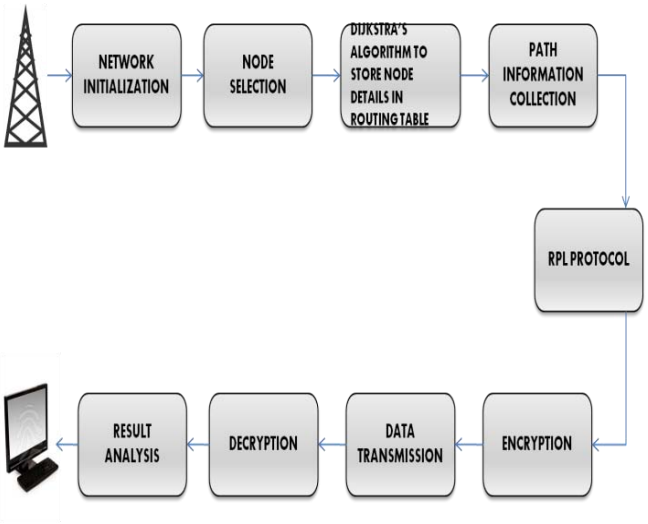

Figure 1: Architecture of Proposed System

B. **Secured data transmission using Blowfish algorithm**: The secured data will be transmitted to its destination node using Blowfish encryption and decryption algorithm and results will be analyzed based on performance (Energy and packet delivery ratio).

In figure 1, the network establishment is followed by selection of communication nodes. The Dijkstra algorithm is used in order to store nodes details in routing table and for routing RPL protocol is used. Finally secured data will be transmitted to destination node and results will be analyzed. The activity diagram for data forwarding is shown in figure 2.

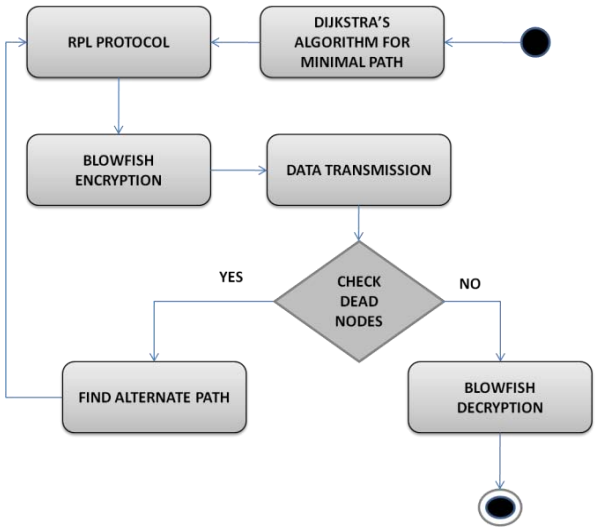

Figure 2: Data forwarding activity diagram

4. Proposed Architecture Instances

4.1 RPL Protocol

The requirements of mesh network for IOT the RPL are developed. The RPL protocol determines in a routing protocol for the needs of IPV6 communications over LLNs. This protocol is find the energy efficient in low-power and lossy networks. RPL is a loop-free distance protocol in which it specifies the minimum amount of energy to find the path that creates routing as a tree and builds a DAG, which divides into a few Destination-Oriented DAGs (DODAGs). In addition, it can be considered as an intelligent directing topology over physical system. For accomplishing necessities of application, it is imperative to choose an arrangement of parameters (steering measurements) that will influence directing choice for each DODAG, these principles is called object function (OF). DAG finds the path according to objective functions (OF) based on Hop-count. In DODAG one of the node is consider as a root which discovers route in the form by upwards and downwards routing to exchange the routing information RPL uses three types of message; Information object (DIO), Destination Advertising object (DAO) and Destination Information Solution (DIS).

DODAG Information Object (DIO): Used to advertise route information those are used to build DODAG.

DODAG Advertisement Object (DAO): DODAG is used to announce the distance between nodes and to transfer the data in a DAG tree.

In this paper, the RPL protocol is implemented to achieve fault tolerance. This protocol aims at forwarding the packets even under faulty node condition by performing a local repair i.e., by choosing an alternative path. The packets are forwarded to destination by means of downward routing mechanism in which the source is fixed. The figure 3 shows the overall flow of RPL protocol.

The Dijkstra‟s algorithm uses the connectivity and distance information among the sensor nodes. The topological information (cost, link in network, connected links) is needed to find out the shortest path between source and destination. By considering the result of productive and iteration the shortest path is calculated.

In this paper, minimal path from one node to the neighboring node is computed using Euclidian distance. The Euclidean distance for any two nodes is given by:

$$d(X,Y) = \sqrt{\sum_{i=1}^{n}(Y_i - X_i)^2} \quad (1)$$

At the first iteration, the algorithm chooses the nearest node among all the neighbor nodes of the source and compute the shortest distance between these two nodes. For the computed nearest node, same procedures repeats till a path is established to the destination.

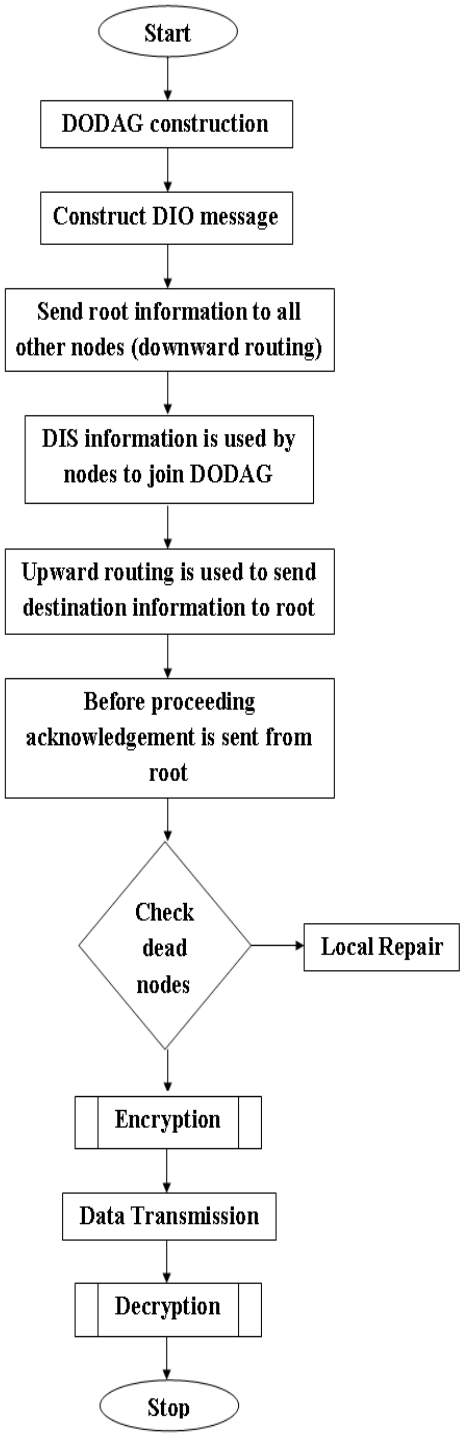

Figure 3: Proposed fault tolerant schema for RPL

4.2 Blowfish Algorithm

Blowfish is one among the fastest algorithms designed for cryptography, which is similar to DES. It is designed from the view of memory and time constraints in a network, which takes 32 bit to 448bits as a variable length key. Blowfish is based on Feistel network with 16 rounds [23]. A function of each round is to compute a data dependent, key dependent and combination key dependent process [22]. To avoid the bit permutations and variable-length shifts, algorithm uses addition, XOR and table lookup.

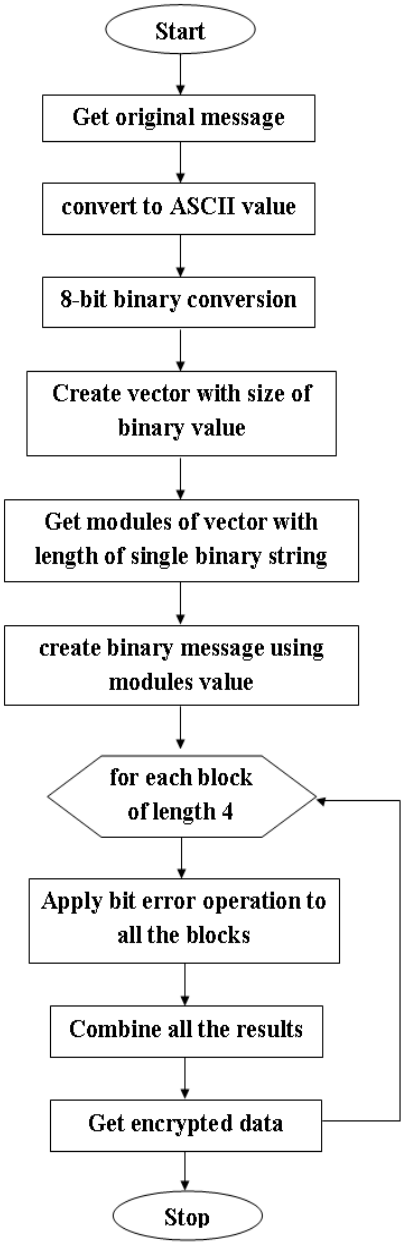

Figure 4: Blowfish Encryption

Blowfish encrypts the data in 64bit blocks which contains two elements, Key expansion (P-arrays) and Data encryption element (four S-boxes). The Blowfish algorithm uses sub-keys to be calculated which prior to encryption and decryption. The simple Pseudo code for blowfish encryption is:

```
for i = 1:4: row
bintext = binMsg(i:i+3,:);
% cip1 = bitxor(key,binMsg(i,:));
cip1 = binMsg (i, :);
cip2 = bitxor (cip1, binMsg (i+1,:));
cip3 = bitxor (cip2, binMsg (i+2,:));
cip4 = bitxor (cip3, binMsg (i+3,:));
Cipher (j, :) = [cip1, cip2, cip3, cip4];
j=j+1;
```

Encryption: In this case, the original message is converted into ASCII values to get 8bit vector binary for encrypt the message. These binary vector values are combined into binary message on each block. The XOR bit operation is applied on each block to get an encrypted data. The figure 4 shows the description of Blowfish encryption.

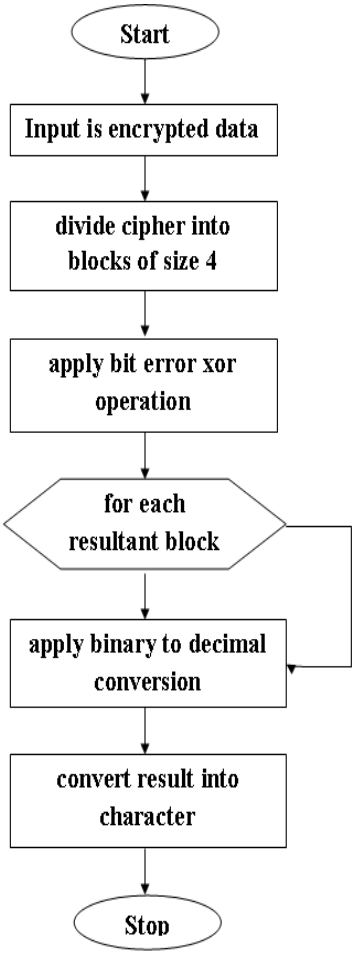

Figure 5: Blowfish Decryption

Decryption: The decryption is done by reversing the encrypted message. By apply the same XOR bit operation on each block to get the result. Finally the binary bit is converted to decimal to decrypt at destination. The figure 5 shows the description of Blowfish decryption.

5. Result Analysis

The simulation of RPL routing protocol is implemented in MATLAB in order to analyze the efficiency of proposed system. The performance is analyzed based on number of nodes. The nodes are scattered randomly in a network. The parameter taken for simulation is listed below in the Table 1.

Table 1: Simulation parameter

Parameter	Value
Simulator	MATLAB(R2010b)
Area	100X100
Number of nodes	20
Data Packet size	512bits
Sensor node position	Static
Data Packet period	2sec

The performance is measured based on two parameters.

Packet delivery ratio- The better packet delivery ratio the correct and complete is the routing protocol.

Energy efficiency- The amount of energy used by a sensor and the vulnerability of each node is consuming the power.

The analysis of the simulation of RPL protocol is done on the performance matrices which are as follows:

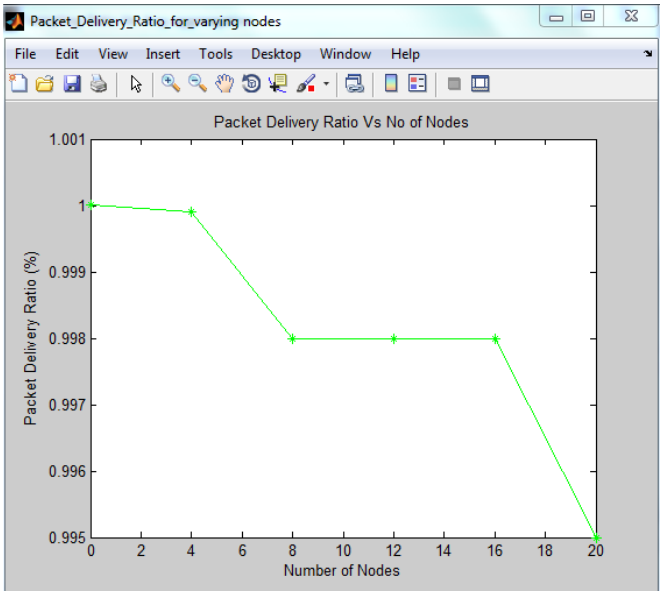

Figure 6: Graph of packet delivery ratio vs. No. of nodes

Figure 6 shows the packet delivery ratio of the network over number of nodes. As the packets are move towards destination for data transmission, if the faults occur in a node then RPL protocol finds the alternative path to transfer a packet.

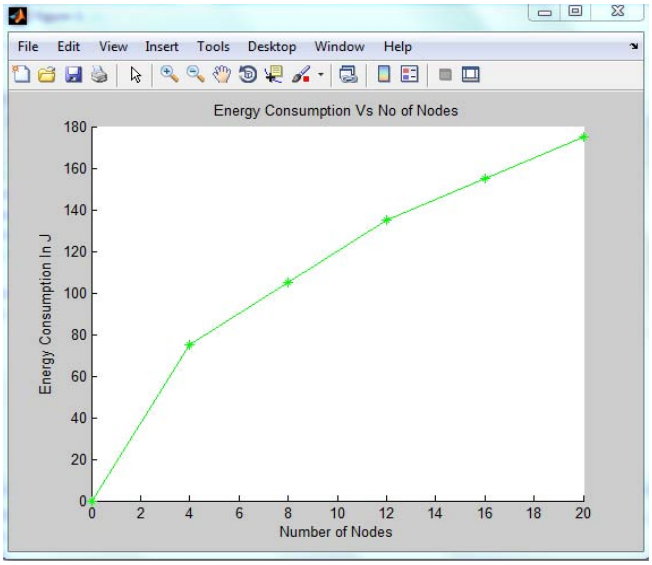

Figure 7: Graph of Energy consumption v/s No. of nodes

Figure 7 shows the energy consumption over the number of nodes. The source routing protocols have a shorter delay because the time taken to discover the route is less and each intermediate hope tries to retrieve information before forwarding the reply. Here the RPL objective function (OF) find the best path that required minimized transmission energy to successfully forward a packet to the destination.

6. Conclusion

The performance evaluation shows the effectiveness of proposed strategy additionally incorporates technique to enhance the security part of WSN. The RPL routing protocol provides minimum amount of energy to find the path for data transmission. The Dijkstra"s algorithm is used to finding the shortest minimal path. The result analysis shows the security structure for successful delivery of packets in the presence of faults. The blowfish algorithm technique that has reconciliation of cryptography in wireless networks that has great perspective in terms of better system security and communication.

References

[1] P. Guillemin and P. Friess, "Internet of Things Strategic research Roadmap", The Cluster of European Research Projects, Technical Report, Sep 2009.
[2] Yi-Bing Lin, Fellow, IEEE, Yun-Wei Lin, Chang-Yen Chih, Tzu-Yi Li, Chia-Chun Tai, Yung-Ching Wang, Fuchun Joseph Lin, Hsien Chung Kuo, Chih-Chieh Huang, Su-Chu Hsu, "EasyConnect: A Management System for IoT Devices and Its Applications for Interactive Design and Art", In proceedings of IEEE Internet of Things Journal, Vol. 5, Issue: 6, 2015
[3] Sudip Misra, P. Venkata Krishna, Harshit Agarwal, anshima Gupta, "An Adoptive Learning approach for Fault –Tolerant Routing in Internet of Things", Wireless Communications and Networking (WCNC), IEEE 2012.
[4] R. Roman, P. Najera and J. Lopez, "Securing the Internet of Things", IEEE Computer, Vol. 44, PP, 51-58, 2011.
[5] Gen Xu, Gang Lu, "Multipath Routing Protocol for DAG-based WSNs with Mobile Sinks", International Conference on Computer Science and Electronics Engineering (ICCSEE), 2013.
[6] Zainab H. Ali, hesham A. Ali, Mahmoud M. Badwy, "Internet of Things (IoT): Definition, Challenges and Recent Research Directions", International Journal of Computer Application", Oct 2015.
[7] Deeksha Jain, p. Venkata Krishna, V. Saritha, " A Study on Internet of Things Based Applications", Networking and Internet Architecture, Cornell University Library, 2012.
[8] Antonio, Angusto Frohlich, Alexandre Massayaki Okazaki, Radrigo Vieira steiner and Peterson Oliveira, "A cross- Layer Approach to Trustfullness in the Internet of Things", International Symposium on Object/component/service-oriented Real-time distributed Computing (ISORC), IEEE 2013.
[9] Qi Jing, Athanasios V. Vasilakos, Jiafu Wan, Jingwei, Dechao Qiu, "Security of the Internet of Things: Perspective and Challenges", Wireless network, Vol. 20, pp 2481-2501, 2014.
[10] Xiong Li, Zhou Xuan, Liu Wen, "Rsearch on the Architecture of Trusted Security System Based on the Internet of Things", International Conference on

Intelligent Computation Technology and Automation (ICICTA), IEEE 2011.
[11] Arbia Riahi , Yacine Challal, Enrico Natalizio, Zied Chtourou, Abdelmadjid Bouabdallah, " A Systemic Approach for IoT Security", International conference on Distributed Computing in Sensor Systems, IEEE 2013.
[12] Sachin Babar, Parikshit Mahalle, Autonietta Stango, Neeli Prasad, Ramjee Prasad, "Proposed Security Model and Threat Taxonomy for the Internet of Things(ioT)", Springer- Verlag Berlin Heidelberg, 2010.
[13] Xin Gu, Jun Yan and Zoujin Huang, "Rsearch on IoT Data Trust Scheme Under Cloud Service Mode", International Conferences on Computational and Information Sciences (ICCIS), IEEE 2014.
[14] Deeapli Deeapli Vermani, "Fault Tolerant Clustering Protocol For Data Delivery in Wireless Sensor Network", International Journal of Future Generation Communication and Networking, Vol.7, No.2, pp.21-34, 2014.
[15] LinusWallgren, Shahid Raza, and Thiemo Voigt, "Routing Attacks and Countermeasures in the RPL-Based Internet of Things", International Journal of Distributed Sensor Networks, Volume 2013, Article ID 794326.
[16] N. Hasan, M. Ali, A. Barradas and N. Correia "Cross-Layer Optimization for Reliability Improvement of Data Delivery in 978-1-4673-7306-7/15/$31.00 c, IEEE 2015.
[17] Prasenjit Chanak, TuhinaSamanta, Indrajit Banerjieu, "Fault-Tolerant Multipath Routing Scheme For Enerfy Efficient Wireless sensor Network", International journal of Wireless and Mobile Networks(IJWAN) Vol. 5, No,2, April 2013.
[18] Attlee M. Gamundani, "An Impact Review On Internet of Things Attacks.", International Conference on "Emerging Trends in Networks and Computer Communications(ETNCC)", IEEE 2015.
[19] Hao Zhang, Ting ting Zhang, "A Peer to Peer Security Protocol for the Internet of Things", "Intelligence in Next Generation Networks (ICIN), IEEE 2015.
[20] Quan Le, Thu Ngo-Quynh, Thomaz Magedanz, "RPL-based Multipath Routing Protocols for Internet of Things on Wireless Sensor Networks", International Conference on Advanced Technologies for Communications (ICATC), 2014.
[21] Leila Ben Saad, Ledric Chauvenet, Bernard Touranchean, "Simulation of the RPL Routing Protocol for IPV6 Sensor Netwroks: Two Case Studies", International Conference on Sensor Technologies and Applications, Sep 2011.
[22] Krishnamurthy G.N, V. Ramaswamy and Leela G.H, "Performance enhancement of Blowfish aggorithm by Modigying its function", "Industrial Electronics and Telecommunication, Springer, 2007.
[23] PiamSingh and Karamjeet Singh, "Image Encryption and Decryption using Blowfish algorithm in MATLAB", International Journal of Scientific & Engineering Research, VOl. 4, Issue 7, July 2013.
[24] Cheng-Rung Tsai, Ming-Chun Hsiao, Wen-Chung Shen, An-Yeu (Andy) Wu, and Chen-Mou Cheng, "A 1.96mm2 Low-Latency Multi-Mode Crypto-Coprocessor for PKC-based IoT Security Protocols", 978-1-4799-8391-9/15/$31.00, IEEE 2015.
[25] Paul Loh Ruen et al., "Cross-Layer Secured IoT Network and Devices", Asia Pacific on Intelligent and Evolutionary Systems (IES), 2014.
[26] Simone Cirani, Gianluigi Ferrari, Luca Veltri, "Enforcing Security Mechanisms in the IP-Based Internet of Things: An Algorithm Overview", Sensor Network, 2013.
[27] Bassam Sharkawy, Ahmed Khattab, Khaled M. F. Elsayed, "Fault-Tolerant RPL Through Context Awareness" ,World Forum on Internet of Things (WF-IoT),IEEE 2014.
[28] Sushruta Mishra et al., "Fault Tolerance in Wireless Sensor Networks", International Journals of Advanced Research in Computer Science and Software Engineering, Vol.2, Issue.10, Oct 2012.
[29] Panagiotis Kartazis et al., "Evaluation of RPL with a transmission count-effiecint and trust-aware routing metric", International Conference on Communication (ICC), IEEE 2014.
[30] Emilio Ancillotti et al., "Reliable Data Delivery with the IETF Rouitng Protocol for Low-Power and Lossy-Networks", IEEE Transactions on Industrial Informatics Vol.10, Issue.3, June 2014.
[31] M. Ali Lodhi et al., "Multiple path RPL for low power lossy networks", Acria Pacific conference on Wireless and Mobile (APWiMob), IEEE 2015.
[32] Mohammed Omer Farooq, "RPL-based routing protocol for Multisink wireless Sensor Network", Wireless and Mobile Computing Networks and Communication (WiMob), IEEE 2015.
[33] Lan Zhang et al., "Intrusion detection system for RPL from routing choice intrusion", International Conference on Communication Workshop (ICCW), IEEE 2015.
[34] Pavan Pongle, Gurunath Chavan, "A survey: Attacks on RPL and 6LoWPAN in IoT", International Conference on Pervalive Computing) ICPC), IEEE 2015