iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** V **Month of publication:** May 2020

DOI: http://doi.org/10.22214/ijraset.2020.5364

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue V May 2020- Available at www.ijraset.com

A Review of Trust based Multicasting Technique for IoT

Jaspreet Kaur[1], Navpreet Kaur[2]
[1]*M.tech Student,* [2]*Assistant Professor, ECE Department, BBSBEC Fatehgarh Sahib, India*

Abstract: ***The trust implementation is fundamentally completely combined with network services in this context or environment (i.e., one should needs to consider whether or not to utilize a service offered by a system based on trust towards the product or device); the principle of trust-based systems integration is of vital importance. Earlier, the RPL routing protocol uses the broadcasting nature for the path establishment from source to destination in which the network bandwidth is very high and also delay for the path establishment is high. In this work the technique of multicasting will be proposed for the path establishment from source to destination. The multicasting technique will be based on the trust mechanism for the path establishment from source to destination. The multicasting technique will reduce the bandwidth consumption and delay in the network. In the trust based routing technique, trust of each node in the network will be calculated based on the number of packets forwarded by any sensor node. The node which forward maximum number of packets in the network had maximum trust.***
Keywords: IoT, RPL, Routing, trust, multicasting, broadcasting.

I. INTRODUCTION

A technology in which several sensors, smart nodes and objects are connected to each other in order to perform communication without using any human efforts is known as the Internet of Things (IoT). Depending upon the link amongst objects, the objects function autonomously. Analysis of gathered data for decision taking, provision of lightweight data and retrieval of data through accessing and approving cloud-based services are some of the actions performed through IoT nodes. Users, programs, detectors as well as the artifacts are tightly connected to each other through IoT. The applications ranging from smart grid healthcare applications to intelligent transport systems deploy IoTs within them. The number of smart devices and intelligent services provided through IoT networks has been outgrowing due to the huge business opportunities provided in the IoT scenarios [2]. The cloud-based IoT networks have been developed due to the relativity of IoT devices on the cloud infrastructure such that the data can be transmitted across applications.

A. Architecture of IoT

Following are the various security requirements defined for each level of IoT architecture:

1) *Perceptual Layer:* Preventing illegal nodes from having access to the systems requires node authentication. It is very important to include data encryption for protecting the confidentiality of information transmission among the nodes [7]. It is important to include advanced key agreement before performing data encryption. However, higher numbers of resources are consumed when stronger safety measures are adopted. Thus, to resolve this issue, the lightweight encryption mechanism is developed in which the lightweight cryptographic protocol and algorithm are included. This research has extended to develop integrity and authenticity of sensor data as well [8].
2) *Network Layer:* It is very difficult to apply existing communication security mechanisms in network layer. The illegal nodes are prevented from entering these layers by applying identity authentication [20]. It is equally important to include confidentiality and integrity within the security approaches applied in this layer. Here, a very commonly found severe attack is the distributed denial of service attack (DDoS). Thus, it is also important for this layer to provide methods through which this attack can be prevented from attacking the vulnerable node.
3) *Support Layer:* Huge application security architecture is required within the support layer. It might include almost all the strong encryption algorithms and encryption protocols, cloud computing and secure multiparty computation, or anti-virus and stronger system security technology to provide secure environments [12].
4) *Application Layer:* It is important to include two different aspects for solving the security related issues of application layer. The first aspect involves the key agreement and authentication in heterogeneous network and the second aspect involves the privacy protection of user. Further, to provide information security particularly with password management, it is very important to include education and management.

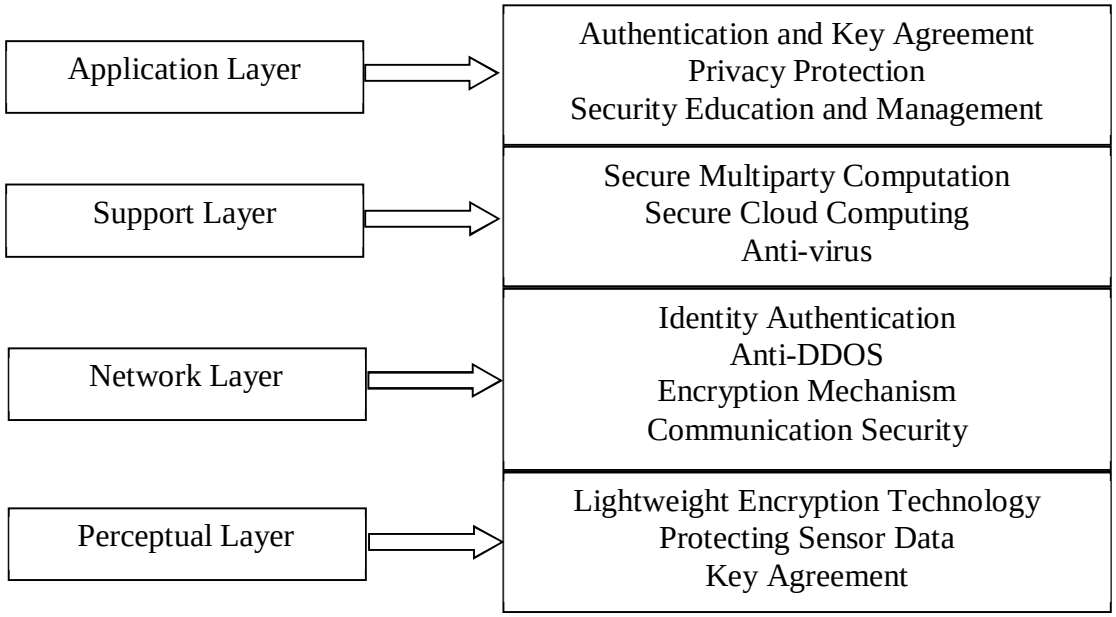


Figure 1.1: Techniques of IoT [25]

B. Routing in IoT

There are mainly IP based web and IoT applications which provide transmission using TCP and UDP. However, among most of the IoT applications [22], there are few commonly used message distribution functions. Various applications implement these functions in interoperable standard ways [9]. Very similar to the client/server protocol, a publish/subscribe protocol architecture is designed which is called MQTT (Message Queue Telemetry Transport). Due to its simple structure and ability to avoid high CPU and memory utilization, MQTT protocol is known to be of huge important.

Another protocol that is designed from the financial industry is the Advanced Message Queuing Protocol (AMQP). The TLS/SSL protocols are used here to manage the security. To ensure that less power and memory embedded devices are being used, CoAP is applied for communication.

Various network layer protocols also have been designed. The most commonly known IoT standard for MAC is the IEEE 802.15.4 [21]. A frame format is defined in this protocol in which the source and destination addresses are defined in headers along with the manner in which nodes can communicate. Low power multi-hop networking is applied lately in IoT because it is not suitable to use frame formats applied previously in traditional networks since they cause overhead in these systems. Channel hoping and time synchronization are used to maintain good efficiency, reduced cost and satisfy IoT communications requirements [6].

II. APPLICATION

There are certain applications in which IoT architectures are being deployed lately. Some of those applications are shown below:

1) *Medical and Healthcare Industry:* The medical parameters and drug delivery of patients are monitored using the cell phone with RFID-sensor capabilities which is one of the several IoT applications of healthcare sector [19]. In case of any accidents, prompt medical attention is required and this is easily provided by IoT systems. The diseases of patients can easily be identified, monitored and prevented by these systems. Also, the records of patients can be stored which can be useful in future emergency conditions through implantable and addressable wireless devices.
2) *Manufacturing Industry:* The optimization of production processes and monitoring of complete lifecycle of objects from production to disposal is possible by linking objects with information technology [15]. This connection can be established either by embedding the smart devices or by using the unique identifiers and data carriers which can be helpful in interaction among the information systems and the intelligent supporting network architecture.
3) *Smart Cities:* For improving the smartness of cities an important role is played by the IoT which helps in monitoring the parking spaces existing in the city, examination of building and bridge conditions and examining the pedestrian levels and vehicles. Further, the sensitive regions of cities, the vehicles levels and adaptive lighting in street lights are monitored through

these systems. Depending upon the climatic conditions and unexpected events occurring in the surroundings various warning messages and diversions are provided to the intelligent highways and smart roads.

4) *Smart Agriculture and Smart Water:* The soil moisture and trunk diameters of vineyards are monitored using IoT systems so that the agricultural field can be improved and strengthened. The amounts of vitamins present in agricultural products are maintained through this monitoring process which can thus result in increasing the growth and production. The fungus and other microbial contaminants which result in causing problems in plants are prevented by controlling the humidity and temperature level. Further, the various environmental conditions are also forecasted easily when IoT systems are deployed [17].
5) *Security & Emergencies:* In this field, the use of IoT technologies has increased to great extent. It is possible to monitor the radiation levels, liquid presence and perimeter access controls in industries to reduce the possibility of disasters. The entry of unauthorized people to restricted regions is detected and controlled by using the perimeter access control mechanism. Any kind of gas leakages and levels within industrial applications and the surroundings of mines and chemical factories are monitored by applying IoT.

III. TRUST BASED TECHNIQUES

There are malfunctioning owners and subsequently misbehaving devices who may conduct unfair assaults for their own benefit depending on their social interactions with others at the detriment of other IoT devices that provide comparable services. In addition, misbehaving nodes that have strong social links will collude and monopolize a class of services [24]. The trust implementation is fundamentally completely combined with network services in this context or environment (i.e., one should needs to consider whether or not to utilize a service offered by a system based on trust towards the product or device); the principle of trust-based systems integration is of vital importance. Trust-based Smart M-IoT approaches can be divided into the following types:

A. Architecture-based Trust in smart M-IoT is attainable through a unique implementation of architecture while placing each entity in such a way that it provides a pathway for believing each other before communications.
B. Decision-based Trust is a decision-based entity, which in some cases is marked by following certain principles of communications. The decision-based trust management mainly has two examples that are node management and selection of next hop.
C. Property-based Trust is itself a property of a device in smart M-IoT. However, this core property may be divided into sub-categories from which trust can be assured across every kind of network.
D. Third-party-based some of the popular approaches in modern day networks are relying on external mode for trust calculations. Such a method utilizes techniques such as deep learning, data mining, neural networks or AI to determine interacting entities trust.

IV. LITERATURE REVIEW

Guo, J. et al. [11], proposed a way to classify trust computation models to-date for IoT systems. The method is to identify current trust computing models supported five design dimensions: trust structure, trust dissemination, trust accumulation, trust upgrade, and trust creation. This work outlines the benefits and drawbacks of the alternatives in each dimension, and illustrates the efficacy in protection mechanisms against targeted hackers. Finally, the gaps in IoT trust computation research were highlighted and future research directions were suggested.

Mayzaud, A. *et al*. [18], presented a unique classification approach for the categorization of the attacks found besides the RPL. Primarily three classes of threats were listed for that strategy. The network's longevity has been shortened by invasions against resources. These attacks generated a plenty of false communication or constructed a number of loops. The implementation and also the management of the security modes were not mentioned by the RPL specification technique. Thus it was inferred that a significant obstacle to the agreed framework of RPL networks was the interaction between various protection rates.

Aris, A. *et al*. [4], presented a deep study of RPL version number attacks. The investigation of the attacks was also performed which was supported different scenarios. The theoretical work was focused on the IETF routing specifications. Only the impact of the invasions of version number on node resource consumption was determined. A probabilistic approach was used to calculate the probabilities for the attacks. The simulation results revealed that the output of the mobile attackers and remote nodes had exactly the same impact on the network. A research should be conducted in the future on the coming actions of DIO knowledge in order to understand the potential role of virtual number threat.

Khan, Z. A. *et al.* [14], proposes some new approaches for IDS which were very suitable for the tiny devices. For managing the status information about the neighbors, the proposed approach used the faith management technique. The proposed approach proved very successful for singling out nastily behaving units. This process was completed in an exceedingly power oriented system. The

most aim of the trust management subjective logic was the recognition of the attacker nodes presented within the system. In this paper, different algorithms have been considered for managing reputation, which are Neighbor Based Trust Dissemination (NBTD), Clustered Neighbor Based Trust Dissemination (CNTD) and Tree Based Trust Dissemination (TTD).

Ma, G. *et al.* [16], Analyzing RPL protection issues, setting up a test network to check RPL network stability, and introducing an M-RPL stability routing protocol based on RPL. The routing protocol defines a hierarchical clustering network topology, the network's intelligent system determines the backup path during the route exploration process in various clusters, enables backup paths to make sure data routing when a network is breached. The test results demonstrate the M-RPL network can withstand the routing assaults successfully. M-RPL offers a way to maintain security over the Internet of Things (IoT).

Santiago, S. *et al.* [23], proposed the planning and implementation of Energy Efficient Routing for IoT. To maximize network efficiency the routing parameters are mixed. The suggested methodology uses fuzzy inference method to blend energy aware metrics to pick the preferred direction and extend the networks' lifespan. The findings are calculated using MATLAB and for the specified scenario the output performance is 63.4 percent.

Abdo, H. *et al*. [1], proposed a novel approach for ensuring the security and safety in case of industrial threat investigation. For this purpose, the newly created variant of protection analysis was paired with a conventionally utilized safety investigation framework named bowtie analysis. The updated version was known as an overview of the attack tree. A new framework was proposed for the estimation of risk scale focused on two term related pieces. The one part was for security while the other part was for safety. The tested results showed that the proposed approach performed well. In future, a more reliable and tough likelihood estimation technique will be developed by the researchers.

Hampiholi, A. S. *et al.* [3], proposed a modified GA called as MEGA (Maximum Enhanced Genetic Algorithm) using Local Search mechanism along with Sleep-Wake up mechanism. It optimizes the Wireless Sensor Network in a way that dynamically results in the energy savings and extension of network lifespan. Design and performance review of ad-hoc networking protocols is carried out utilizing software-based modeling methods, and device functionality is tested for different networking situations and WSN environments with increased energy conservation and routing capacity.

Elappila, M. *et al.* [10], proposed a protocol in the real time network where the traffic is more and also congested by so many data sources sending their packets to the base station at the same time. Around the same time, the protocol chooses the route with a strong survivability rating, thus attempting to pick the one that has fewer resistances from the other nodes as well as the environment. Our algorithm uses a criterion for choosing the next hop node, which is a feature of the signal-to-interference-noise-ratio of the connection among these two, survivability parameters of the route from that node to the destination, and the trip-loss distance from that node to the destination. Aris, A. *et al.* [5], proposed two simple alleviation approaches for the elimination of RPL version number attacks. Changes to the version number from the path of the leaf nodes were removed with the first mitigation strategy. The first solution offered details about the durability of the sites for virtual number. In the second method, nodes may adjust their virtual number only when the mass number of nearest nodes with better rankings reported a modified virtual number. The efficiency of the proposed approach was verified by using a number of topologies. In future, more experiments can be performed in the area of various virtual number invasions scenario.

Jaiswal, K. *et al.* [13], proposed an Optimal QoS-aware multipath routing protocol for IoT based Wireless Sensor Networks. The proposed scheme defines the path from source to destination by calculating the ideal cost factor, taking into account two factors, i.e. lifetime and node overcrowding. While this protocol embraces two kinds of packet control, it provides fewer energy usage and better QoS. Extensive simulation has been done and a particular routing algorithm has been compared to the current state of the art to help improved efficiency of the proposed protocol.

V. RESEARCH METHODOLOGY

The RPL routing protocol uses the broadcasting nature for the path establishment from source to destination. Due to broadcasting nature of RPL routing protocol, the network bandwidth is very high and also delay for the path establishment is high. In this work, the technique of multicasting is proposed for the path establishment from source to destination. The multicasting technique will be based on the trust mechanism for the path establishment from source to destination. The multicasting technique will reduce the bandwidth consumption and delay in the network. In the trust based routing technique, trust of each node in the network will be calculated. The trust of each node in the network is calculated based on the number of packets forwarded by any sensor node. The node which forward maximum number of packets in the network will be considered as the cluster head node. The cluster head node will receive the route request messages and nodes which are responsible to establish path to destination. The path from source to destination will be established which have minimum hop count and maximum sequence number.

The trust of each node in the network will be calculated based on the number of packets forwarded by any sensor node in the network. The node which forward maximum number of packets in the network had maximum trust. The trust defines the reliability of the sensor node. The sensor node which is maximum reliable through that node path from source to destination will used for data transmission.

As illustrated in figure 5.1, the network will be deployed with the finite number of sensor nodes. The source and destination nodes will be defined in the network. The data will be forwarded from source to destination. The whole network will be divided into clusters with location based clustering. The trust of each node will be calculated based on the number of packets forwarded into the network. The sensor node which forward maximum number of packets will have maximum trust value. The sensor nodes which have maximum trust value will be selected as the cluster head. The cluster heads will forward information to base station

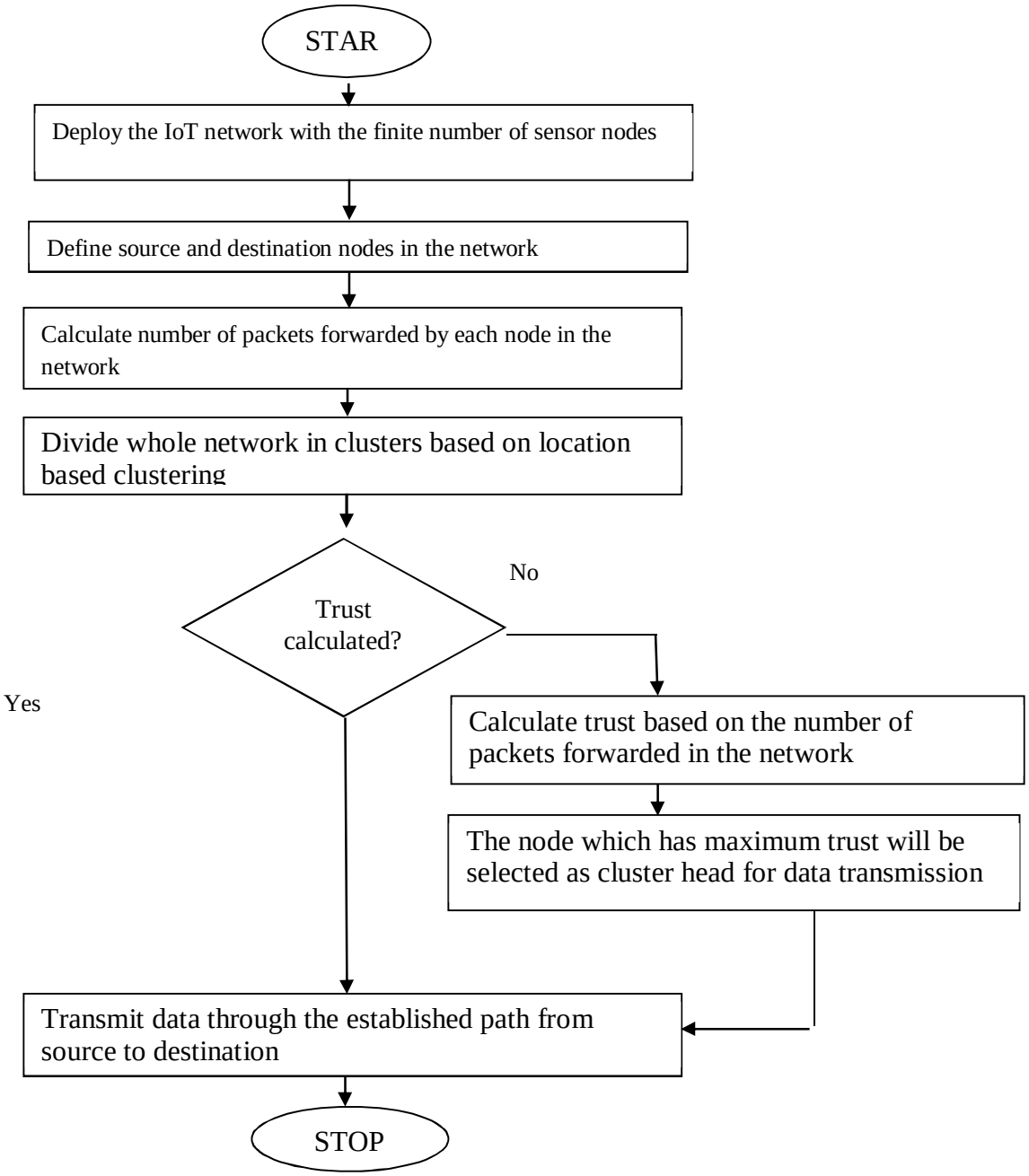


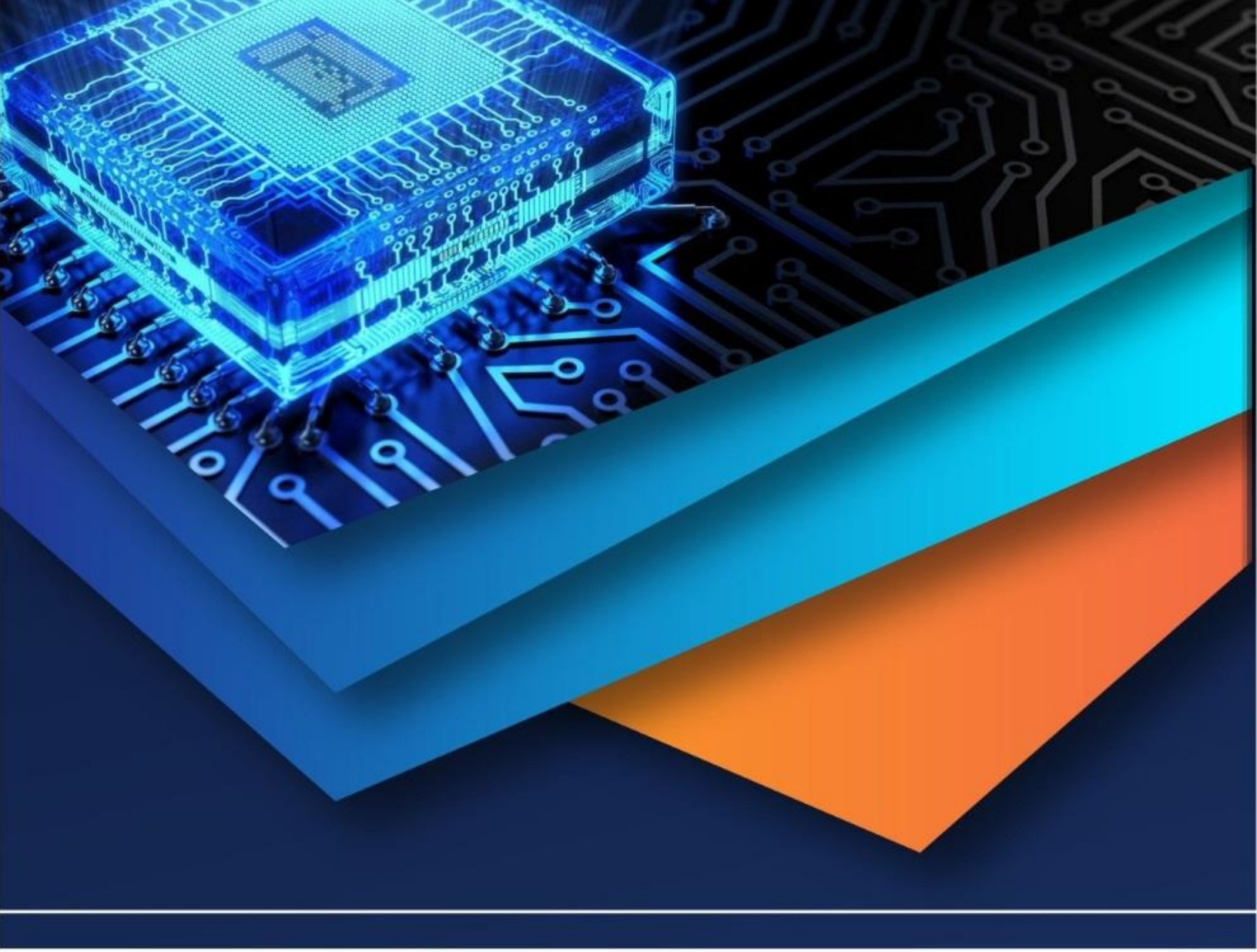
Figure 5.1 Research Methodology

VI. CONCLUSION

There are malfunctioning owners and subsequently misbehaving devices who may conduct unfair assaults for their own benefit depending on their social interactions with others at the detriment of other IoT devices that provide comparable services. While trust provisioning is inherently fully integrated with network services in this environment, the idea of trust-based service management is of utmost importance. The RPL routing protocol uses the broadcasting nature for the path establishment from source to destination. The broadcasting techniques for the path establishment like DODAG consume high network bandwidth which affects network performance. The DODAG (Destination Oriented Directed Acyclic Graph) is the routing algorithm for the path establishment but it is not able to recover the path from source to destination. When the link failure happened in the network, it will increase delay in the network. The multicasting technique is proposed that is based on the trust mechanism for the path establishment from source to destination. The multicasting technique will reduce the bandwidth consumption and delay in the network. The trust of each node in the network is calculated based on the number of packets forwarded by any sensor node and the node which forward maximum number of packets in the network had maximum trust.

REFERENCES

[1] Abdo, H. Kaouk, M. Flaus, J. M. and Masse, F. “A safety/security risk analysis approach of Industrial Control Systems: A cyber bowtie – combining new version of attack tree with bowtie analysis,” Comput. Secur., vol. 72, pp. 175–195, 2018.
[2] Abdul-Qawy, A. S. Pramod, M. P. E. and Srinivasulu, T. “The Internet of Things (IoT): An Overview,” J. Eng. Res. Appl. , vol. 5, no. 12, pp. 71–82, 2015.
[3] Aishwarya, S. Hampiholi, B. P. Kumar, V. “Efficient routing protocol in IoT using modified Genetic algorithm and its comparison with existing protocols”, 2018 3rd International Conference on Circuits, Control, Communication and Computing (I4C)
[4] Aris, A. Oktug, S. F. and Yalcin, S. B. O. “RPL version number attacks: In-depth study,” Proc. NOMS 2016 - 2016 IEEE/IFIP Netw. Oper. Manag. Symp., no. Noms, pp. 776–779, 2016.
[5] Arış, A. Yalçın, S. B. Örs and Oktuğ, S. F. “New lightweight mitigation techniques for RPL version number attacks,” Ad Hoc Networks, vol. 85, pp. 81–91, 2019
[6] Baccelli, E. Philipp, M. and Goyal, M. “The P2P-RPL Routing Protocol for Ipv6 Sensor Networks: Testbed Experiments,” SoftCOM 2011, 19th Int. Conf. Software, Telecommun. Comput. Networks, Split, vol. 1, pp. 1–6, 2011.
[7] Bandyopadhyay D. and Sen, J. “Internet of things: Applications and challenges in technology and standardization,” Wirel. Pers. Commun., vol. 58, no. 1, pp. 49–69, 2011.
[8] Bhuvaneswari V. and Porkodi, R. “The internet of things (IoT) applications and communication enabling technology standards: An overview,” Proc. - 2014 Int. Conf. Intell. Comput. Appl. ICICA 2014, pp. 324–329, 2014.
[9] Chakrabarti, A. “Emerging Open and Standard Protocol Stack for IoT,” AVP Digital Practice, vol. 1, no. 1, pp. 2–6, 2015.
[10] Elappila, M. Chinara, S. “Dynamic Survivable Path Routing for Fast Changing IoT Network Topologies”, 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)
[11] Guo, J. Chen, I.-R. “A Classification of Trust Computation Models for Service-Oriented Internet of Things Systems”, 2015 IEEE International Conference on Services Computing
[12] Hopalı E. and Vayvay, Ö. “Internet of Things (IoT) and its Challenges for Usability in Developing Countries,” vol. 2, no. January, pp. 6–9, 2018.
[13] Jaiswal, K. Anand, V. “An Optimal QoS-aware multipath routing protocol for IoT based Wireless Sensor Networks”, 2019 3rd International conference on Electronics, Communication and Aerospace Technology (ICECA)
[14] Khan Z. A. and Herrmann, P. “A trust based distributed intrusion detection mechanism for internet of things,” Proc. - Int. Conf. Adv. Inf. Netw. Appl. AINA, pp. 1169–1176, 2017.
[15] Luzuriaga, J. E. Cano, J. C. Calafate, C. Manzoni, P. Perez, M. and Boronat, P. “Handling mobility in iot applications using the mqtt protocol,” in Internet Technologies and Applications (ITA), pp. 245–250, IEEE, 2015.
[16] Ma, G. Li, X. Pei, Q. Li, Z. “A Security Routing Protocol for Internet of Things Based on RPL”, 2017 International Conference on Networking and Network Applications (NaNA)
[17] Mayzaud, A. Badonnel, R. and Chrisment, I. “A distributed monitoring strategy for detecting version number attacks in RPL-based networks,” IEEE Trans. Netw. Serv. Manag., vol. 14, no. 2, pp. 472–486, 2017.
[18] Mayzaud, A. Badonnel, R. and Chrisment, I. “Detecting version number attacks in RPL-based networks using a distributed monitoring architecture,” 2016 12th Int. Conf. Netw. Serv. Manag. CNSM 2016 Work. 3rd Int. Work. Manag. SDN NFV, ManSDN/NFV 2016, Int. Work. Green ICT Smart Networking, GISN 2016, pp. 127–135.
[19] Posegga, J. Eder, T. Nachtmann, D. Parra, D. and Schreckling, D. “Real Life Security (5827HS) Trust and Reputation in the Internet of Things Trust and Reputation in the Internet of Things,” Conference Seminar SS2013, pp. 1–19, 2013.
[20] Pote, S. V. “Internet of Things Applications , Challenges and New Technologies,” vol. 67, no. 978, pp. 45–51, 2018.
[21] Ren, W. “QoS-aware and compromise-resilient key management scheme for heterogeneous wireless Internet of Things,” International Journal of Network Management, vol. 21, no. 4, pp. 284- 299, 2011.
[22] Salman T. and Jain, R. “Networking protocols and standards for internet of things,” Internet Things Data Anal. Handb., vol. 1, no. 1, pp. 215–238, 2017.
[23] Santiago, S. Arockiam, L. “A novel fuzzy based energy efficient routing for Internet of Things”, 2017 International Conference on Algorithms, Methodology, Models and Applications in Emerging Technologies (ICAMMAET)
[24] Sharma, V. You, I. Andersson, K. Palmieri, F. Rehman, M. H. “Security, Privacy and Trust for Smart Mobile-Internet of Things (M-IoT): A Survey”, Networking and Internet Architecture, 2019.
[25] Suo, H. Wan, J. Zou, C. and Liu, J. “Security in the internet of things: A review,” Proc. - 2012 Int. Conf. Comput. Sci. Electron. Eng. ICCSEE 2012, vol. 3, pp. 648–651, 2012.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY