# Trust Mechanism in IoT Routing

**Sridhar Manda, Nalini N**

***Abstract:*** ***The word "thing" is a device, Internet is nothing but interconnection, so we can define IoT as the set of objects interconnected together with the network to share the information. A route is needed to share this information while sending data from one device to another device the network route or data can be attacked, to avoid this attacks a device trust mechanism is a useful mechanism to reduce data loss. In this paper, it's discussed that what are the various routing attacks can be occurred in IoT, and how to avoid these attacks by using trust mechanism, later results shown how data loss is reduced with trust mechanism.***

***Keywords: IoT, routing, trust, routing attack, trust mechanism.***

## I. INTRODUCTION

Now a day's Internet of Thing is an emerging technology a lot of research is going on to make the world technically very strong. This will make the human being how to work easily. Today everybody wants to do the smart work they want to sit in a place and operate or work effectively. We can define internet of thing as a set of devices which are uniquely identified in a network and having an ability to share or transfers the information with or without human interaction. In the real world, many devices are connected together these devices growing up every day. As per the statistics portal surveys there were many devices (estimated) are connected worldwide from 2015 to 2020. This survey is made from around 22,500 sources. This survey shows that in 2015 the number of devices are around 15.41 billion devices by 2017 its increased to 20.35 billion devices and by 2020 it may grow up to 75.44 devices [3].

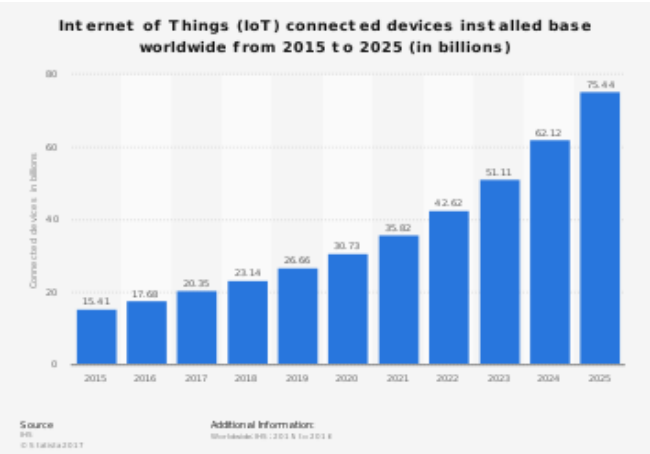


**Figure 1: IoT connected devices from 2015-2025 [3]**

While the number of devices increasing every day more data will be shared among the devices. When there is huge data is shared among devices then there must be high chances of data attacks. This paper discusses the IoT architecture, the types of attacks in each phase, trust mechanism to avoid attacks.

## II. IOT ARCHITECTURE AND ATTACKS

Internet of thing architecture is built up with six layers these layers named as Multilayer, Application layer, Transport layer, Network layer, Data link layer, Physical layer. Figure 2 shows the multilayered structure of IoT.

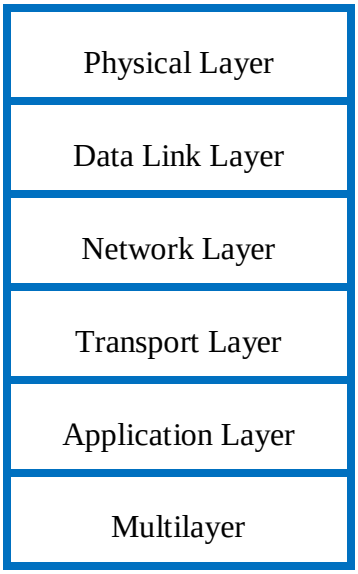


**Figure 2: IoT Multilayered Architecture**

IoT architecture consists of a set of layers these layers are used to establish the communication and shares the data with devices. In this architecture, there are six layers the first one is the physical layer which consists of the physical objects like Sensors, RFID [1], smart objects, etc. These devices gather information from the environment and also identify other objects. Next layer is data link layer used to transfers data between the nodes in a network and also detects the errors occurred in the physical layer. Data link layer uses a set of IoT protocols to transfers data from one node to other nodes. The network layer is used to identify other smart devices or servers, it also used to transfer and process data of sensors. Physical layer gathers information this data is stored and processed then this processed data is transferred to an application layer, this processed data transformation is done in Transport layer. Transport layer transfers the processed data from the physical layer to the application layer.

**Revised Manuscript Received on March 10, 2019.**

**Sridhar Manda**, Research Scholar, Computer Science, University of Mysore, Karnataka, India.

**Dr. Nalini N**, Professor, CSE NITTE Research and Education Academy, Karnataka, India.

The Application layer is used to provide application related services to the users. Internet of things can be deployed by defining various applications. Example for this is smart homes, smart healthcare system etc. Multilayer used to manage the whole system.

## III. IOT LAYERS AND ATTACKS

This section explains about the attacks in each layer. The multilayer consists of set nodes these nodes are managed for providing quality of service. While the set of nodes are working in the network some nodes may be attacked with the "Denial of Service attack [9]" and "Man-in-Middle attack [10]". The application Layer is used to provide services to users so while providing this services code can be attacked or the reliability of the node may be damaged. Application layer can be attacked with the "Reliability Attack" and "Malicious code attack". Transport Layer is used to transfer data to the application layer. In transport Layer, we may get three types of attacks like "Data Integrity Attack", "Energy Drain Attack", "Desynchonization Attack".Network Layer is used to identify other devices and servers so here in this layer we may get attacks like "Spoofing attack", "Black hole attack [4]", "Sinkhole attack [2]", "Sybil attack [5]", "Node replication attack", "Wormhole attack [6]", "Hello flood attack [7]". Data Link Layer uses set of protocols to transfer data while transferring data we may get different attacks like "Jamming attack", "Collision attack". Physical layer gathers information from different devices like sensors, RFID's etc. while in physical layer we may get different attacks like "Eavesdropping attack", "Node tampering attack".

## IV. TRUST

A trust is defined as believing in the nodes service, i.e. a source node sends data to other whenever if it believes that the receiving node is not harmful, authenticated, no data loss, not attacked, and finally if it's safe. Trust can be divided into three parts; i) trust based on behavior: this is nothing but expectation of a participant behavior; ii) trust based on computation: trust between the agents in a network like sensors in a network; iii) trust based on technology: in the form of security technology establishing trust and evaluating trust between devices in IoT[11]. We will consider three parameters to trust a device those parameters are [-1, 0, +1], these are taken like when a node indicated with +1 then we can say it is trusted, if it is -1 then it's completely destruct, and finally if its 0 then more data is needed to take a decision. Internet of things consists of a set of devices communicated each other via a network to exchange information. In this, we have source node (sender) and the destination node (receiver) in between many other nodes may exist. A route is established between the devices for communication [8]. A device in IoT is energy constrained node, so node energy is calculated based on four parameters those are: data transmission, data receiving, device idle, and device sleep. The total energy consumption of a device is calculated based on packet receiving, sending, this can be expressed as

$$E_{te} = E_t + E_r + E_i \qquad (1)$$

Here $E_{te}$ is total energy of a node, $E_t$ is energy consumption for data transmission, $E_r$ is energy consumption to receive data, $E_i$ and is energy consumption for node idle. So the total energy consumption of a node is calculated by the sum of transmission, receive and idle. A parameter of node energy depends on the time factor. i.e.

$$E_t = P_t * T,\ E_r = P_r * T, E_i = P_i * T \qquad (2)$$

Here $P_t$ is packet transmission, $P_r$ packet receiving, $P_i$ is idle and T is the time taken for transmitting a packet.

In IoT a sender node sends authenticated data packet on the network, another node receives a packet while receiving it also authenticates the packet this authentication depends on the trust value. Here it's taken that $T_{tr}$ refers to the level of node's trust associated with $P_r$ and $P_t$ . Nodes authentication is decided by taking the function.

**Algorithm for receive procedure:**

1. Function Receive(m, $P_t$)
2. Condition is if(f($T_{tr}$)) true
3. Then send (m, nextHop)
4. Otherwise
5. Condition if(Authenticate(m)) true
6. Then send(m, nextHop)
7. Otherwise
8. Drop_pack(m)
9. End all conditions
10. End function

## V. TRUST CALCULATION

The trust level $T_{tr}$ associated with $P_r$ and$P_t$. This trust is value taken as a real number between 0 and 1 where 0 indicated no trust and 1 indicates trust. To calculate trust level $P_r$ depends on three components those are $E_{tr}$ its experiences, $O_{tr}$ its observations, and $R_{tr}$ its recommendations are taken for $P_t$ . Then the above consideration trust value is calculated as

$$T_{tr} = \alpha E_{tr} + \beta O_{tr} + \gamma R_{tr} \qquad (3)$$

Where $\alpha, \beta, \gamma$ are weighing factors, these factors keep a value of trust between zero and one. i.e $\alpha + \beta + \gamma = 1$. Here the three components are calculated and the first one $E_{tr}$is calculated based on the trust level taken from the experience between 2 nodes. When $P_r$ receives a packet from the $P_t$ based on the function it decides whether it is authenticated or not. If the received packet is authenticated then $E_{tr}$ becomes positive otherwise its keeps unauthenticated message.

Experience of the two node calculated by using the following equation

i.e $E_{tr} = \delta^e E'_{tr} + (1 - \delta^e) \times aval$ aval=0,1,x

Here in this equation $E'_{tr}$ means old experience value, so based on this the new experience calculated. That is new value depends on the old value and exact experience value. $\delta^e$ Is a parameter used to keep experience value between 0 and 1. If experience value is 0 then the message is authenticated and trusted, if its x then the message is unauthenticated and untrusted. $O_{tr}$ is calculated based on the trust level taken by the nodes behavior observations. If $P_t$ transfers data to other node $P_r$ then this node must forward data to other node without modifying data. A node transmits data to other nodes without data modification when that packet is authenticated. If it's an unauthenticated packet the $O_{tr}$ will be decreased.

A network nodes behavior based on observations is calculated as the following equation

i.e $O_{tr} = \delta^e O'_{tr} + (1 - \delta^e) \times aval$ aval=0,1,y

Here in this equation $O'_{tr}$ means old observation value, so based on this the new observation value is calculated. That is new value depends on the old value and exact experience value. $\delta^e$ Is a parameter used to keep observations value between 0 and 1. If the new observation value is 0 then the message is authenticated and trusted, if its y then the message is unauthenticated and untrusted. Otherwise observation value becomes zero. $R_{tr}$is calculated as when $P_r$ receives recommendations from $P_k$ about $P_t$then it updated its recommendation factor $R_{tr}$.

## VI. AUTHENTICATION FUNCTION

A packet is transferred from$P_t$, this packet authentication is decided by the authentication function f based on trust value$T_{ij}$. In a network a set of node were there for these nodes we take the threshold value. When a malicious node found in the network, then that node continuously sends wrong packets to other node and recommends accepting that packets and it convince the neighbor node to accept packets then $T_{ij}$ exceeds the threshold of $P_r$ , then $P_r$ never authenticate transferred packet. Then automatically no value of trust component will be changed so it will not trust the given packet. From this figure 3 shows the simulation result for finding the malicious node.

**Authentication Function Algorithm**

1. Function f($T_{tr}$)
2. Then condition if($T_{tr} < th$)
3. Then return false
4. Otherwise
5. If($period_j = 0$) then
6. $period_j = random()\%q_j$
7. Return false
8. Otherwise $period_j = period_j - 1$
9. Then return true
10. End conditions
11. End of function

In the above algorithm $period_j = random()\%q_j$ used to select a node randomly. If the $T_{tr}$ is less than threshold then received message is unauthenticated otherwise it an authenticated message. If it's an unauthenticated message then it's a malicious node and continuously sends wrong messages.

## VII. SIMULATION PARAMETERS

**Table 1: simulation parameters**

| Parameters | Value |
|---|---|
| Simulation time | 40 |
| No. of nodes | 16 |
| Simulation range | 149 |
| Simulation area | 300×500 |
| Trust intervals | 10 |

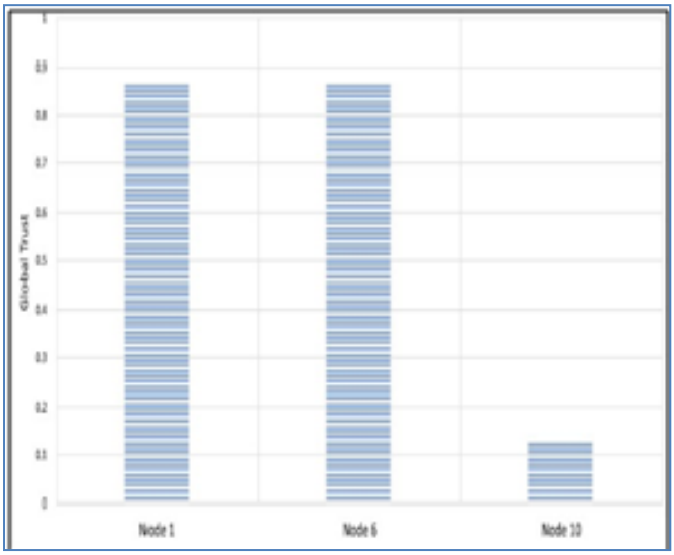


**Figure 3: Detection of malicious node**

In this simulation node 1 and node 6 gives feedback because these two nodes were trusted node but node 10 acts like a malicious node so this node drops number of packets and always gives a negative feedback so we can find node 10 as a not trusted node. Then this system changes the route when such malicious node found in the given network with the trust value.

## VIII. CONCLUSION

In Internet of Things securing the route and securing the data sends from source to destination is the main task. So for this the suitable mechanism in the "trust" this is used to protect the route as well as the data. Here in this paper by using this trust mechanism it found the simulation results how to avoid the packet loss whenever a malicious node found. In this system when a malicious node find immediately that node is not trusted based on the taken parameters and immediately if will selects other trustee nodes. By this, we can reduce the packet loss rate.

## REFERENCES


1. Jaroslav Kadlec*, Radek Kuchta, Radovan Novotný and Ondřej Čožík. (2014), "RFID Modular System for the Internet of Things (IoT)", Industrial Engineering & Management. Vol.3 issue 4.
2. Raju Stephen, Dalvin vinoth Kumar. (2016). Deist: Dynamic Detection of Sinkhole Attack For Internet Of Things. International Journal of Advanced Trends in Computer Science and Engineering. 5 (12), 19358-19362.
3. The Statistics Portal "Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions)" © Statista 2018.
4. Neelam Janak Kumar Patel1 , Dr. Khushboo Tripathi2. (2017). Analysis of Black Hole Attack in MANET Based on Simulation through NS3.26. International Journal on Recent and Innovation Trends in Computing and Communication. 5 (5), 194-205.
5. Kuan Zhang, Xiaohui Liang, Rongxing Lu, Xuemin Shen. (2014). Sybil Attacks and Their Defenses in the Internet of Things Sign In or Purchase. IEEE Internet of Things Journal. 1 (5), 372-383.
6. International Journal of Engineering and Technical Research (IJETR). (2017). Detecting And Monitoring Wormhole in IoT enabled WSNs Using EyeSim. Nilima Nikam, Poorna R. Pimpale, Pranali Pawar, Anita Shirture. 2 (6), 15-17.
7. Virendra Pal Singh1 , Sweta Jain2 and Jyoti Singhai3. (2010). Hello Flood Attack and its Countermeasures in Wireless Sensor Networks. IJCSI International Journal of Computer Science. 3 (11), 23-27.
8. Nasreen Fathima1 Dr. Reshma Banu2 Dr. G. F. Ali Ahammed3. (2017). A Comparative Study Of Routing Approaches For Energy Constrained Devices In Iot . International Journal Of Current Engineering And Scientific Research (Ijcesr). 4 (1), 47-52.
9. Krushang Sonar 1 , Hardik Upadhyay 2 . (2014). A Survey: DDOS Attack on Internet of Things. International Journal of Engineering Research and Development. 10 (11), 58-63.
10. Christian Simko. (2016). Man-in-the-Middle Attacks in the IoT. https://www.globalsign.com/en/blog/man-in-the-middle-attacks-iot/.
11. "Securing consumer trust in the internet of things", Principles and Recommendations 2017.
12. Internet of Things (IoT) Trust Concerns, Jeffrey Voas, Rick Kuhn, Phillip Laplante, Sophia Applebaum, October , 2018, NIST Cybersecurity White Paper.