SHARE DECISIVELY! AN ALGORITHM FOR RELIABLE COMMUNICATION IN IOT NETWORK

PRIYA J[1], VINOTHINI C[2], PAVITHRAD[3]

[1]Department of Information Technology, [2]Department of Computer Science and Engineering,

[3]Department of Electronics and Communication Engineering,

[1]Bannari Amman Institute of Technology, [2]Dr.N.G.P. Institute of Technology,

[3]Sri Ramakrishna Institute of Technology, Tamilnadu

[1]priyaajothimani@gmail.com, [2]vinuchidambaram@gmail.com,

[3]pavimba07@gmail.com

Abstract. Sharing of information with third parties intrinsically incurs major risk and heads to distinctive security and privacy issues, which drags the reliability of the entire network system. The buzzing technology, Internet of Things comes under the ubiquitous computing includes sensing, analyzing and controlling with the help of sensors and actuators. The Security of a network would be the greater importance to be considered in wireless communication systems. A potty eavesdropping can result in IoT network failure. The proposed algorithm named *ERA* (Enhanced Reliability Algorithm) provides a procedure to improve the reliability of communication inside the IoT network in terms of secured data transmission. Henceforth, the algorithm comes under a trust based enhancement scheme which guaranties the data must be safe and decisive.

Keywords: IoT, Security, Trust, Reliability

1 Introduction

Internet of things: the technology attracts people from all walks of life with its greatest efficiency and the way it makes daily life easier. Though it leads the growth in application development, it lags in the implementation part of the same. Why, because there is no assurance provided in terms of security, privacy, scalability and reliability to anyone as given in the Fig.1. For most of the IoT applications, the transmission of collected information must be reliable and indispensable. Such types of applications confide on IoT devices operating above wireless communication channel which are innately unreliable [1].

The major difference between Internet of Things and other long-existing communication techniques is that the data transmission and communication in IoT network has no human participation. Since there is no human intervention, IoT communications has critical problems in reliability and security more than any other existing challenges that hamper the deployment of applications in large scale environment.

Additionally, all the sensor data and actuators instructions have to retain reliability to secure against modifications in the transactions. Thus, Reliability is one of the elementary requirements for whatever the type of network via wireless communication.

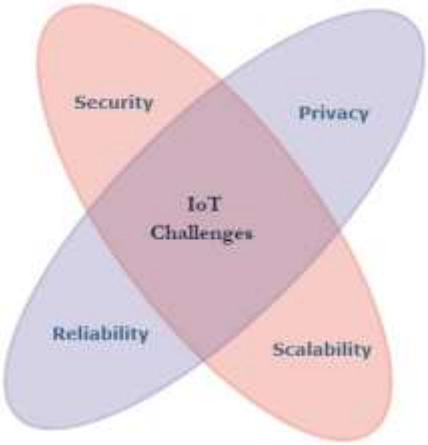

Fig.1 IoT Challenges

A short remainder of this paper follows as: The Architecture of IoT communication is figured in section 2. Section 3 describes the need for reliability in network communication. Problem formulation and the proposed algorithm are explained in section 4. Whereas section 5, the Conclusion which precedes References.

2. IoT Communication Architecture

The architecture given in Fig.2 provides an outline of the communication flow of the system, components used, as well as the description of the system.

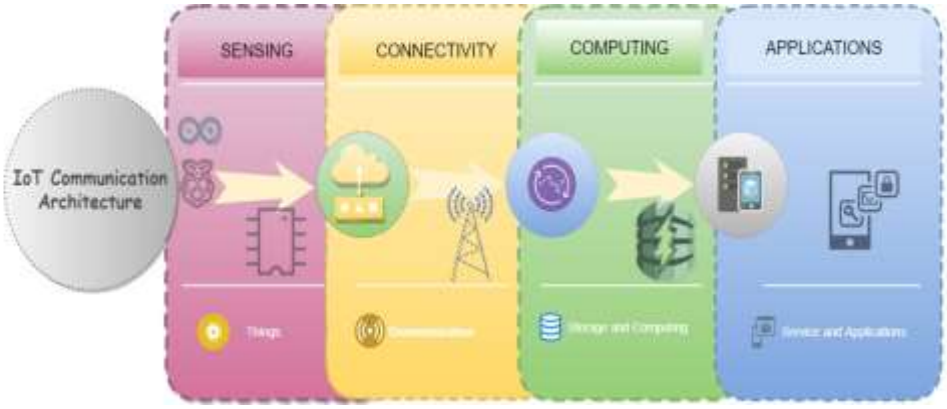

Fig.2 Architecture of IoT Communication

The above mentioned architecture comprises of,

- **Sensing:** “Things’ like sensors, actuators, controller are the prominent devices in IoT used for sensing and transmits the required information
- **Connectivity:** Next step after sensing is transmission of data via “Internet”. Connection between nodes to be established for transmission.
- **Computing:** Received information should be computed and get stored in a database for further process.

- **Applications:** Here, the destiny of all the above steps comes to an end. Applications are the end product of IoT in every walk of life.

Thus, the construction of layers in IoT communication model is as common as in most of the communication paradigms. The difference among technologies should be based on its efficiency and performance. In that case, the IoT is one of the best technologies in terms of all aspects except the one *"security"* which is the foremost essential aspect to be concerned. A lot many researches are still going on to resolve the issues and challenges in IoT and to make it as "the best technology" for all. As a potty contribution to it, an algorithm is framed in this paper for improving reliability in data sharing across the IoT networks.

3. Need for Reliability

The reliability of a network model signifies the possibility that the system will perform a task without a failure within a stipulated period of time considering physical devise failures, data loss and attacks. One of the challenges in the IoT environment is reliability without human intervention, in accord with long-distance transmissions, intermediary routing, and wireless interfering and sniffing attacks. Also, if invaders can categorize and compromise sensors and actuators involved in the network, they can certainly spoils actuator directions to terminate IoT controls [2][3].

Reliability is an acute concern for IoT communication, since unreliable data transmission leads to faulty observing data reports, long delays, and data loss, makes the network down. Hence, extraordinary reliable communication is mandate for any type of the network in the future generation communication schemes. Data reliability and security are key elements for a network that operates over wireless communication where the sensed data and actuators information are sharing among all the nodes from each entity across a network is going to be got compromised or ruined.

By considering the usage factors of each service for all the nodes that presents in a network, the performance of a network also the reliability can be defined as discussed in (Network Service). While using the protocols or schemes like mean time to repair (MTTR), meantime between failure (MTBF), very reliable routing protocol (VRRP) the relative impact of reliability in a network could be improved [4] rapidly that improves the increasing in development and deployment of products based on IoT used by all sort of consumers, small and large industries and so on. Therefore, reliability must be taken into an account of consideration hardware as well as software and all aspects of the network terminals [5]. The term reliability is also defined as follows, the pd (partial derivative) of data reliability with respect to the reliability of an entity or a "thing" in the network. To establish a significant evaluation strategy for assessing QoS of a product, reliability also play a role in it [6].

4. Proposed Algorithm

Considering 'n' number of sensors 's_i' get connected with an IoT network. For authenticity, every device to be registered based on any one of the authenticity algorithm in prior and get their unique device ID 'D_i'. Another parameter called 'trust' indicates the probability of a sensor or a device that gets compromised by an attacker and generates fake reports. These device IDs and the trust values are retained in a table and that table [D, Trust] is maintained by an actuator or a controller.

The value of trust is calculated by using two metrics, one is number of verification failures occurred and another is number of fake ID deletions. Verification failure happens if there is a mismatch in hash values between the sender and receiver. In this check, the trust value is also known. For that, as a first step, identify the nearest device, actuator or sensor by using its ID. Use mean median technique to find out the most existed IDs that are near to the controlling device or actuator as a result, calculate the number of devices around and check for the hash values among the nodes for verification. If the verification is get cleared by a device is termed as genuine. Make the genuine devices' ID as a list and get stored in a variable.

Table 1. ERA: Enhanced Reliability Algorithm

Algorithm:- ***ERA: Enhanced Reliability Algorithm***

```
Require: s[1],s[2],….,s[n]
Ensure: Result
s[1],s[2],….,s[n]<=Sort(s1,s2,….,sn)
Result[1] <= s[(n+1)/2
Partition s[1],s[2],….,s[n] into sets with the same value.
for (i = 1 to n) do
    for (j = i + 1 to n) do
      if (s[I]!=0 AND s[j]==s[I]) then
      s[j] <= 0
      T[I]<=T[I]+1
end if
end for
end for
Find the largest T[I]
for (i = 1 to n) do
   if (t < T[I]) then
    T <= T[I]
    L <= i
end if
end for
Result[2] <= s[L]
b <= Average( s[1],s[2],….,s[n])
for (i = 1 to n) do
D[I]<=(s[i]-b)^2
end for ….

    …..
    Find the least D[I]
    for (i = 1 to n) do
    if (D>D[I]) then
    D <= D[I]
    L<=i
    end if
    end for
    Result[3] <= s[L]
    Actuator returns corresponding ID for a given
value by checking the packet fields
    for i = 1 to 3 do
    getID [i] <= GiveID(Result[i])
    end for
    Find the largest getID[I] in trush table
    for (i = 1 to 3) do
    if (trust < Trust[i] ) then
    trust <= Trust[i]
    L <= i
    end if
    end for
    Result <= Result[L]
```

Here, the number of fake ID deletions is directly proportional to the number of entity get compromised. The calculations mentioned here are denoted in the algorithm proposed. Based on that, the factual the exact devices have been identified. By using any one of the mathematical scheme identify the devices or nodes that are nearest to the actuator or controller among others. Then and as a result delete or remove the device IDs which are out of the range in the network while doing calculation. Assign a parameter to the final result of this identification. Now, two parameters are there that holds the information about the genuine device/node/user ID of the IoT network. Thus, data transaction and sharing of information would happen between these genuine IDs. Therefore, the communication between nodes across the network becomes safe and secure. By the way, the data reliability gets improved.

5. Conclusion

The proposed ERA algorithm provides a procedure to improve the reliability of communication in IoT network in terms of secured data transmission. Integrity and Confidentiality also attained by using this algorithm, among the users. Unreliable data transmission leads to faulty observing data reports, long delays, and data loss, makes the network down. Extraordinary reliable communication is mandatory. Therefore, trust in terms of reliability builds in the IoT network and attains completeness. This proposed algorithm comes under a trust-based enhancement scheme that guaranties the data must be safe and decisive.

6. References

1. Z. Ali, Z. H. Abbas, and F. Y. Li, “A stochastic routing algorithm for distributed IoT with unreliable wireless links,” *IEEE Veh. Technol. Conf.*, vol. 2016-July, 2016, doi: 10.1109/VTCSpring.2016.7504110.
2. W. Ren, L. Yu, L. Ma, and Y. Ren, “RISE : A ReIIable and SEcure Scheme for Wireless Machine to Machine Communications,” vol. 18, no. 1, pp. 100–107, 2013.
3. J. Priya and M. Gunasekaran, “Security-Aware and Privacy-Sensitive of Internet of Things (IoT) : A Review.”
4. M. Vogt, R. Martens, and T. Andvaag, “Availability modeling of services in IP networks,” *Proc. - 4th Int. Work. Des. Reliab. Commun. Networks Des. Manag. Highly Reliab. Networks Serv. DRCN 2003*, pp. 167–172, 2003, doi: 10.1109/DRCN.2003.1275353.
5. P. Phister and D. Olwell, “Reliability , Availability , and Maintainability.”
6. K. Tokuno and S. Yamada, “User-perceived software service availability modeling with reliability growth,” *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 5017 LNCS, pp. 75–89, 2008, doi: 10.1007/978-3-540-68129-8_8.
7. S. S. Prasad and C. Kumar, “A Methodology for an Efficient and Reliable M2M Communication,” Int. J. Soft Comput. Eng., no. 3, pp. 2231–2307, 2013.
8. A. Mathur, T. Newe, W. Elgenaidi, M. Rao, G. Dooly, and D. Toal, “A secure end-to-end IoT solution,” Sensors Actuators, A Phys., vol. 263, pp. 291–299, 2017, doi: 10.1016/j.sna.2017.06.019.
9. J. Xin, L. Guo, N. Huang, and R. Li, “Network service reliability analysis model,” Chem. Eng. Trans., vol. 33, no. 2011, pp. 511–516, 2013, doi: 10.3303/CET133308.
10. X. Li, J. Niu, S. Kumari, F. Wu, A. K. Sangaiah, and K. K. R. Choo, “A three-factor anonymous authentication scheme for wireless sensor networks in internet of things environments,” J. Netw. Comput. Appl., vol. 103, pp. 194–204, 2018, doi: 10.1016/j.jnca.2017.07.001.
11. S. R. Moosavi et al., “End-to-end security scheme for mobility enabled healthcare Internet of Things,” Futur. Gener. Comput. Syst., vol. 64, pp. 108–124, 2016, doi: 10.1016/j.future.2016.02.020.
12. I. Romdhani, Existing Security Scheme for IoT. Elsevier Inc., 2017.