Journal of Critical Reviews TRUST-BASED DATA PROTECTION AND AUTHENTICATION TECHNIQUE FOR IOT- SENSOR NETWORKS

Article *in* Journal of Critical Reviews · May 2020

DOI: 10.31838/jcr.07.07.129

CITATIONS
0

READS
60

2 authors:

K. Kavitha
Guru Nanak College
7 PUBLICATIONS **31** CITATIONS

SEE PROFILE

Suseendran G.
VELS INSTITUTE OF SCIENCE, TECHNOLOGY & ADVANCED STUDIES (VISTAS), CHENNAI.
149 PUBLICATIONS **1,211** CITATIONS

SEE PROFILE

Journal of Critical Reviews

ISSN-2394-5125 Vol 7, Issue 7, 2020

TRUST-BASED DATA PROTECTION AND AUTHENTICATION TECHNIQUE FOR IOT-SENSOR NETWORKS

[1]K. Kavitha, [2]Dr.G. Suseendran

[1]Ph.D. Research Scholar,Department of Computer Science VELS Institute of Science, Technology & Advanced Studies Assistant Professor, Chellammal Women's College Chennai, India
Email: kavi.thirumal13@gmail.com
[2]Assistant Professor,Department of Information Technology School of Computing Sciences,VELS Institute of Science, Technology & Advanced Studies Chennai, India.
Email : suseendar_1234@yahoo.co.in

Received: 14.02.2020 *Revised: 18.03.2020* *Accepted: 22.04.2020*

Abstract
In IoT environments, sensor nodes often need to transfer a massive quantity of identified data to the doorway in a petite duration. Therefore the door needs to usually validate the collaborating strategies in every period. But traditional security methods which involve cryptographic operations and privacy protections are not applicable in IoT networks, due to their resource constraints. Hence we propose to design trust-based data protection and authentication technique for IoT-WSN. In this technique, the behavioral trust and data trust values of each device are estimated by the data aggregator. Then, a total trust value is derived for each device using both types of these trust values. During data aggregation, the aggregator omits the data from the tools, whose trust values are low. To protect the data and perform authentication, a ticket-based message authentication code (MAC) is applied by the IoT sender. Simulation results show that the proposed technique involves a higher delivery ratio with reduced energy consumption.

Keywords:Internet of Things (IoT), Sensor networks, Authentication, Message Authentication Code (MAC), Trust, Aggregator

DOI: http://dx.doi.org/10.31838/jcr.07.07.129

INTRODUCTION

The Internet of Things (IoT) is globally expanding, providing many profits in nearly every phase of life. This network can be utilized to connect wireless sensors and radio frequency identification (RFID) for reliable transmission. It links people and belongings to data systems through smart devices centered on Internet concerned strategies and information patterns. It consists of various devices belonging to smart cities, intelligent houses, supply chains, and agriculture. In the areas of transport and industries, IoT plays a vital role in terms of huge commercial benefits [1].

Safety and secrecy issues encounter the IoT apparition. A huge sum of facts will be made from billions of exchanges amid strategies and people. In this situation, mischievous devices may achieve prejudiced occurrences centered on faith exploitation. As many of the identifying strategies organized in an IoT ambiance are physically available by opponents, the physical safety of device hardware and data safety for device communications have turned out to be stern apprehensions for the disposition of IoT structure [2].

The safety concerns of IoT milieus comprise information defense, admittance control, and device confirmation. In specific IoT milieus, sensor nodules ought to often diffuse a massive quantity of identified data to the doorway in a petite duration. Therefore the door needs to recurrently validate the collaborating devices in every period [3].

But traditional security methods which involve cryptographic operations and privacy protections are not applicable in IoT networks, due to their resource constraints. Hence integrating security solutions in IoT should result in reduced power consumption and overhead [4].

Our previous work [11] proposed a priority-based adaptive scheduling algorithm (PASA) for IoT sensor systems. In this work, time slots are allotted for nodes based on traffic priority to avoid collisions. The sleep period of each node was dynamically adjusted based on traffic priority, queue size, residual energy, and transmit power.

In our work [12], a technique for maintaining reliability and consistency in data collection for IoT-WSN is developed. In this technique, a set of candidate nodes is selected based on the energy eligibility factor and buffer space availability. Once the data is sensed at a time interval, it is checked for consistency. If the information is consistent, then it will be transmitted to the selected candidate node, which aggregates the data and transmits towards the sink. At the sink, the packet error rate (PER) is estimated. If it is high, each source will send the replicated data to a selected set of K candidate nodes.

Trust denotes the honesty of devices during communication. It is the process of constructing a cordial relationship between the tools of the network. Hence as an extension to these works, we propose to design trust-based data protection and authentication technique for IoT-WSN.

Related Works

An intelligent trust computation model [5] based on ML has been developed. In this model, a multi-class SVM technique is used to classify the trustworthy interactions and malicious interactions. To group the interactions, K-Means clustering is applied. However, since it involves both unsupervised and supervised learning techniques for detecting honest transactions, it requires enormous computational complexity.

Patil Abhijit et al. [6] have suggested a faith-based exemplary for giving the safety at the application layer. With the aid of previously intended prototypes and resolutions stated in the literature survey, they are suggesting a Faith exemplary, which will function as Trust based Safe Fog Ecosystem for haze and IoT centered uses. By putting on appropriate Verification majors, Appropriate Admittance Control Approaches, Frivolous Crypto-graphic algorithm-based data encryption (If obligatory), and

Faith focused data communication will progress the complete safety of the IoT and Haze nodules.

Hela Maddar et al. [7] have proposed a novel interference discovery exemplary for IoT WSNs. This excellent belief on a topographical position of the nodules to ensure that we interconnect with the correct bud for every deal. Consequently, they suggested procedures for perceiving doses.

Mufti Mahmud et al. [8] have introduced a Neuro-Fuzzy centered Brain-inspired trust management model (TMM) on protecting IoT devices and on guaranteeing data dependability. The suggested TMM uses nodule developmental faith and data faith assessed by means of Adaptive Neuro-Fuzzy Implication System and weighted-additive approaches correspondingly to evaluate the node's reliability.

Ing-Ray Chen et al. [9] have proposed and examine a 3-tier cloud-cloudlet-device ranked trust-based amenity organization called IoTHiTrust. Their mobile cloud ranked amenity organization etiquette permits an IoT client to bang its service skills and enquire its biased service faith notch toward an IoT service supplier after a climbable report-and-query enterprise. They led a prescribed scalability investigation along with an ns-3 replication presentation investigation signifying that IoT-Hi Trust not only attains scalability deprived of negotiating exactness, merging, and resiliency belongings against malevolent bouts but also outdoes current disseminated and federal IoT faith organization etiquettes.

Zeeshan Ali Khan et al. [10] have proposed a trust-based method for handling the trust of each IoT device of the network. Based on the trusted nodes, a Low power and Lossy networks (RPL) routing protocol is designed.

Proposed Solution

Overview

In this technique, the behavioral trust (BT) value of each device is estimated by the data aggregator based on the data forwarding rate, packet dropping rate, and interaction success rate. It then estimates the data trust (DT) values based on the absolute differential value (estimated in [12]) and remaining battery capacity. Finally, a total trust value is derived for each device using BT and DT values by the aggregator. During data aggregation, the aggregator omits the data from the devices, whose trust values are low. To protect the data, a simple message authentication code (MAC) is applied by each sender.

Trust Estimation

Behavioural Trust

Data Forwarding Rate (DFR)

The DFR of a node N_j is given by the ratio of number of packets forwarded by N_j to the total number of packets received by node N_j

$$DFR_j = \frac{No\_FWD_j}{No\_REC_j} \quad (1)$$

Packet Dropping Rate (PDR)

The PDR of node N_j at the network layer is given by the ratio of several packets dropped by node N_j to the total number of packets received by node N_j.

$$PDR = \frac{No\_DRP_j}{No\_REC_j} \quad (2)$$

Interaction Success Rate (ISR)

It is estimated based on interaction frequency (F), period of interaction (Z) and no. of successful interactions (C_{succ}).

$$ISR_j = \sum_{m=1}^{F} Z / C_{succ} \quad (3)$$

$$BT_j = DFR_j, + PDR_j + ISR_j \quad (4)$$

Data Trust

The absolute differential value (D) is defined as the relative difference between the present and previously obtained measurements, which is given by

$$\mathbf{A}DF = \begin{cases} If\ A = \mid Q_t - Q_{(t-1)} \mid > \alpha, & 1 \\ Otherwise & ,0 \end{cases} \quad (5)$$

Where α is the threshold value, Q_t and Q_{t-1} are the current and previous sensor measured values.

$$DT_j = ADF \quad (6)$$

Total Trust

Precisely, the trust grade of a provided nodule N_j signified by T_j is assessed by summing up the developmental and data trust using the succeeding Eq.

$$T_j = w_1.\ BT_j + w_2.\ DT_j \quad (7)$$

Where w1 and w2 are the weight values such that w1+w2=1

Trust based attack detection

During data aggregation, the aggregator omits the data from the devices, whose trust values are low.

Let T_{th} be the threshold value of trust maintained for each device by the aggregator. Let S_i be the IoT sender, and AGG_i be its corresponding aggregator.

The trust based attack detection algorithm is given below:

Algorithm

1. For each sender S_i
2. Do
3. S_i transmits the data to AGG_i
4. AGG_i collects BT values of S_i from its neigbors
5. AGG_i estimates DT values of S_i
6. AGG_i computes total trust value T_i of S_i
7. If $T_i < T_{th}$, then
8. S_i is suspected as an attacker
9. AGG_i drops the data packets from S_i
10. End if
11. End For

Data Protection

Authentication is performed for the period of data broadcast from the sensor nodule to the aggregator AGG_i at time T.

Assumptions

Let S be the sender, and AGG_i be its corresponding aggregator.
Let ID_S be the ID of the sender S
Let DP be the data packet generated at S.
Let TK_{IS} be the initial ticket possessed by the sender S.
Let r and m be random numbers generated at S and AGG_i
Let HMAC be the message digest of DP

Algorithm: Authentication and Data Protection

1. S masks the data packet by computing

$$y = DP \oplus H((TK_{IS} \oplus m) \| r)$$

2. S computes message digest as

$$M = HMAC_{TK_{IS}}(ID_S, y, r)$$

3. S transmits Z=[ID_S, M, y, r] to AGG_i
4. If AGG_i receives Z, then
5. AGG_i sets the current timestamp value as T_{cur}
6. If (T_{cur}-T_s)>=T), then
7. Ts is out of range of the period T.
8. AGG_i first computes

$$y' = (m \| TK_{IS}) \oplus H(TK_{IS} \oplus r) \| m)$$

9. AGG_i then computes the ACK as

$$ACK = H((m \| TK_{IS}))$$

10. AGG_i transmits (ACK,y') to S
11. End if
12. End if
13. AGG_i retrieves the initial ticket TK_{IS} of ID_S from its database
14. AGGi computes

$$y_1' = y \oplus H((TK_{IS} \oplus m) \| r)$$

$$M' = HMAC_{TK_{SN}^{I}}(ID_S, y, r)$$

15. If M' = M, then
16. DP is not modified
17. Else
18. DP is fabricated
19. Discard DP
20. End if

The IoT sender has stored initial token TK_{IS} for the current verification period T. Then, the dispatcher uses the arbitrary number m, which had been created to calculate y for hiding the identified data. After that, the sensor node computes the message digest M in order to detect that the message has been modified during data transmission. Next, the sender transmits *ID_S, M, y*, and *r* to AGG_i.

Upon receiving these values from the sender, the AGG_i achieves a sequence of confirmation errands. Initially, AGG_i fixes the present timestamp value as t_c. Then, it confirms whether the conventional message is created in the current verification time *T*. If t_c is out of array of T, the AGG_i calculate y' and ACK. Then, AGG_i directs ACK and y' to the dispatcher.

After verifying the timestamp, AGG_i verifies the data integrity of the message. Based on the received *ID_S*, AGG_i obtains the corresponding initial token TK_{IS} from its database. It then computes y_1 and M' respectively. Then AGG_i confirms whether the calculated value *M'* is corresponding to the current value *M. If* both are identical, it designates that the found message is not altered for the period of the broadcast. Otherwise, the word is considered as fabricated, and hence it is discarded by the aggregator.

Simulation Results

Simulation Parameters

The simulation of TDPA is conducted in NS2, and it is compared with the Time Difference Of Arrival' (TDOA) [7] and Trust-based Resilient Routing (TBRL) [10] technique.

The simulation parameters are shown in Table 1.

Table 1 Simulation parameters

Size of the network	21 to 101
Size of the Area	50m X 50m
MAC layer	IEEE 802.15.4
Simulation Time	50 sec
Traffic Source	CBR
Number of attacker	2
Rate	50Kb

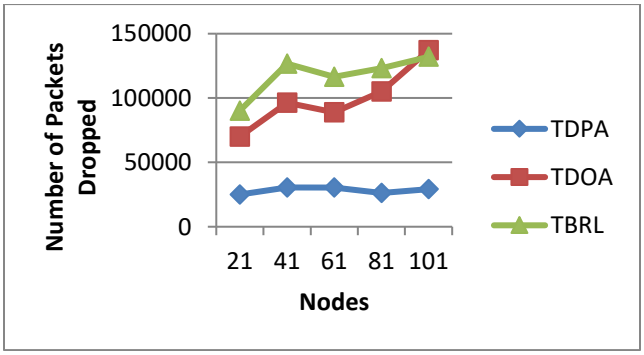

Figure 1 Number of packets dropped

Figure 1 shows the number of packets dropped for all three schemes. As per the figure, TBRL has the lowest packet drop, followed by TDOA and TBRPL, with the highest packet drop. Since TDPA avoids both internal (packet drop) as well as external (fabricating) attacks, it has a 74% reduced packet drop than TDOA and a 79% reduced packet drop than TBRL.

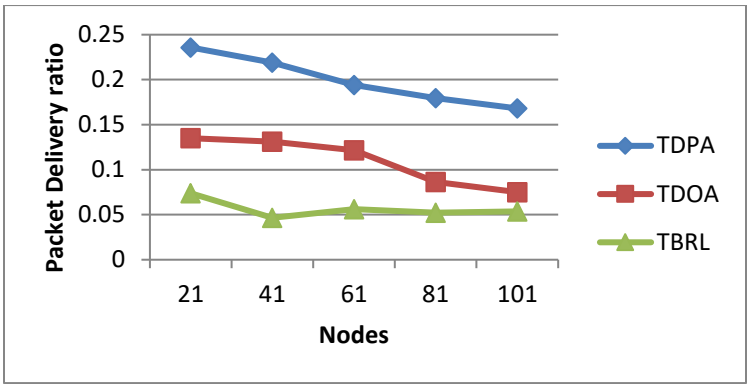

Figure 2 Packet Delivery Ratio

Figure 2 shows the packet delivery ratio measured for all three schemes. As per the figure, TBRL has the lowest delivery ratio, followed by TDOA and TDPA with the highest delivery ratio. Since TDPA avoids both internal (packet drop) as well as external (fabricating) attacks, it has a 41% increased delivery ratio than TDOA and a 64% increased delivery ratio than TBRL.

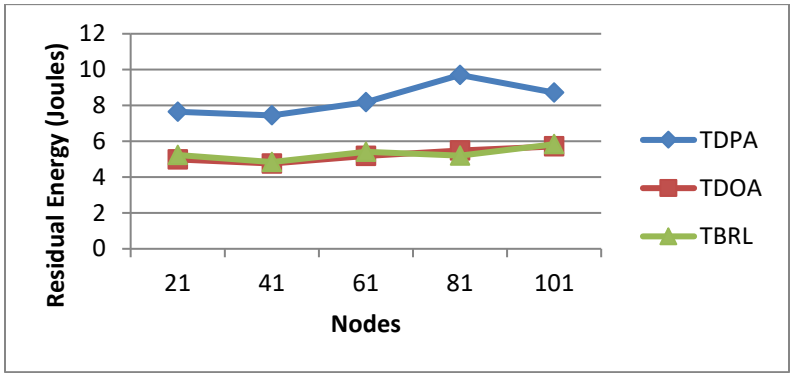

Figure 3 Average Residual Energy

Figure 3 shows the average residual energy measured for all three schemes. As per the figure, TBL and TDOA have similar values of residual energy, whereas TDPA with the higher residual energy. Since TDPA selects energy-efficient aggregators, it has 37% increased residual energy than TDOA, and 36% increased residual energy than TBRL.

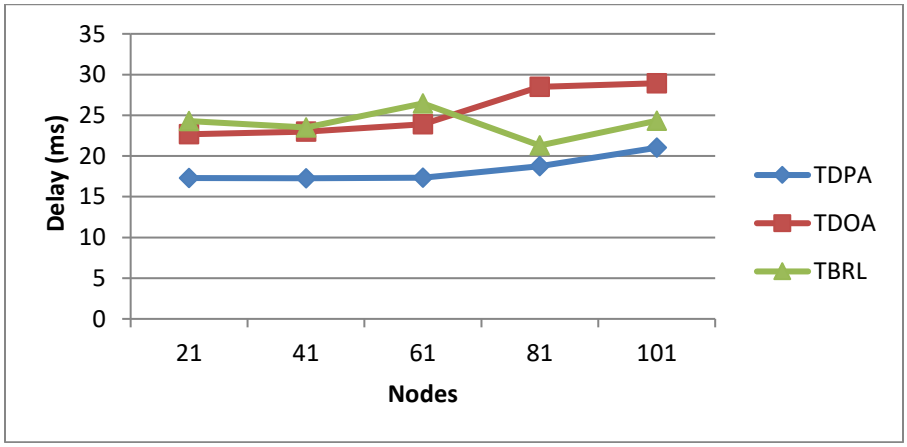

Figure 4 End-to-End delay

Figure 4 shows the end-to-end delay measured for all three schemes. As per the figure, TDPA has the lowest delay, followed by TBRL and TDOA with the highest delay. Since TDPA omits the untrusted devices, it has a 34% reduced delay than TDOA and 33% reduced delay than TBRL.

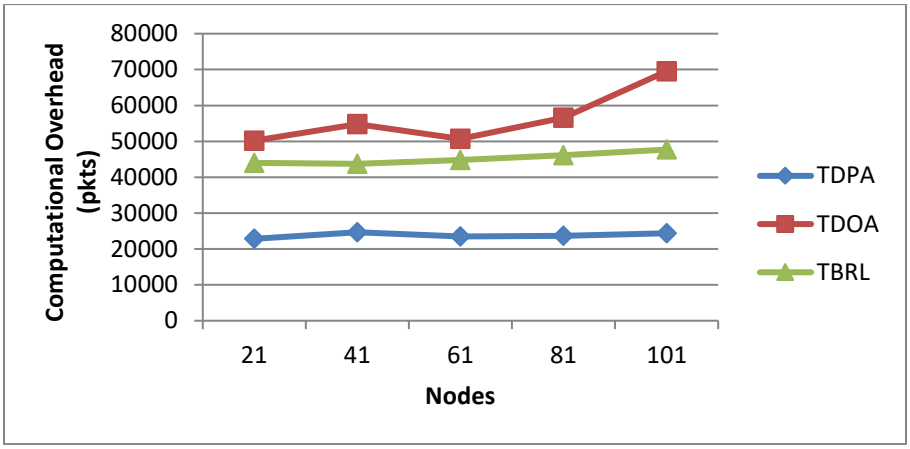

Figure 5 Computational overhead

Figure 5 shows the computational overhead measured for all the three schemes. As per the figure, TDPA has the lowest overhead, followed by TBRL and TDOA, with the highest overhead. Since TDPA uses lightweight MAC scheme for protection, it has 64% reduced overhead than TDOA, and a 56% reduced overhead than TBRL.

CONCLUSION

In this work, a Trust-based Data Protection and Authentication technique (TDPA) for IoT-WSN has been designed. In this technique, the behavioral trust and data trust values of each device are estimated by the data aggregator. Then, a total trust value is derived for each device using both types of these trust values. During data aggregation, the aggregator omits the data from the devices, whose trust values are low. To protect the data and perform authentication, a ticket-based message authentication code (MAC) is applied by the IoT sender. The simulation of TDPA is conducted in NS2, and it is compared with the TDOA technique. Simulation results show that the proposed TDPA involves a higher delivery ratio with reduced energy consumption and overhead.

REFERENCES

1. Yair Meidan,Michael Bohadana,Asaf Shabtai,Martin Ochoa,Nils Ole Tippenhauer,Juan David Guarnizo and Yuval Elovici, "Detection of Unauthorized IoT Devices Using Machine Learning Techniques",arXiv:1709.04647v1 [cs.CR] 14 Sep 2017.
2. Jean Caminha ,Angelo Perkusich and Mirko Perkusich, "A Smart Trust Management Method to Detect On-Off Attacks in the Internet of Things",Security and Communication Networks,Volume 2018,pp:1-10,2018.
3. Suman Sankar Bhunia and Mohan Gurusamy, "Dynamic Attack Detection and Mitigation in IoT using SDN",27th International Telecommunication Networks and Applications Conference (ITNAC),2017.
4. Mahzad Azarmehr, Arash Ahmadi and Rashid Rashidzadeh," Secure Authentication and Access Mechanism for IoT Wireless Sensors
5. Upul Jayasinghe, Gyu Myoung Lee, Tai-Won Um, Qi Shi,"Machine Learning based Trust Computational Model for IoT Services", IEEE TRANSACTIONS ON SUSTAINABLE COMPUTING, TSUSC, 2017
6. Patil Abhijit J and G. Syam Prasad, "Trust based security Model for IoT and Fog based Applications", International Journal of Engineering & Technology, 7 (2.7) (2018) 691-695.
7. Hela Maddar, Wafa Kammoun, Habib Youssef, "Effective distributed trust management model for Internet of Things", Elsevier,Procedia Computer Science 126 (2018) 321–334,2018.
8. Mufti Mahmud, M. Shamim Kaiser, M. Mostafizur Rahman, M. Arifur Rahman,Antesar Shabut, Shamim Al-Mamun and Amir Hussain, "A Brain-Inspired Trust Management Model to Assure Security in a Cloud based IoT Framework for Neuroscience Applications",Cognitive Computation,https://doi.org/10.1007/s12559-018-9543-3.
9. Ing-Ray Chen, Jia Guo,Ding-Chau Wang,Jeffrey J.P. Tsai,Hamid Al-Hamadi and Ilsun You, "Trust-based Service Management for Mobile Cloud IoT Systems",IEEE,2018.
10. Zeeshan Ali Khan,Johanna Ullrich,Artemios G. Voyiatzis and Peter Herrmann, "A Trust-based Resilient Routing Mechanism for the Internet of Things",ACM,2017.
11. Kavitha K., Suseendran G., "Priority Based Adaptive Scheduling Algorithm for IOT Sensor Systems", IEEE Xplore, July 2019, pp.361-366.
12. Kavitha .K, G.Suseendran G., "A Review on Security Issues of IOT Based on Various Technologies", Journal of Advanced Research in Dynamical and Control Systems, Vol.10 (4), June, 2018, pp.
13. Suseendran G, Sasi Kumar A, "Secure Intrusion-Detection System in Mobile Adhoc Networks", Indian journal of Science and Technology, Volume 9, Issue 19, May 2016. pp.1-6