TOPSIS Based Ranking System for Heterogeneous Nodes in IoT

R. Thiruk Kumaran, P. Muthu Kannan

Abstract: The Internet of Things is an innovative approach and has made a substantial effect on both industrial and human's professional life. It aims to increase the ubiquity of the internet and communication between heterogeneous devices and human beings with smart intelligence in a distributed manner. This requirement cannot be well managed by the existing security protocols because of the limited storage space and computation resources. Various threats have significant advantage using trust management scheme. However, it requires some other scheme to secure data in the IoT network. Nodes are having different communication technologies, different energy level, and different computing capacity and so on. This paper presents the Trust Based Cluster Head Selection using TOPSIS for IoT (TBCHS-T) for heterogeneous environment. It uses trust value, Residual Bandwidth Ratio (RBR), and Packet Receiving Delay (PRD) parameters to identify best node among neighbors and the same one is elected as cluster Head. The selection of energy, bandwidth and delay is highly desirable parameter for heterogeneous nodes in IoT. Furthermore, the inclusion of trust value will achieve selection of secured cluster head. The performance comparison between fuzzy logic based trust aware access control system (TAACS-FL) and TOPSIS based TBCHS is analyzed by using Network Simulator (NS-2). From the result it is evident that TBCHS-T has been achieved better improvements in terms of network performance and secured communication compared with TAACS-FL.

Index Terms: IoT, Security, Cluster Head, Access Control, Trust, TOPSIS.

I. INTRODUCTION

IoT system interconnects sensors, machines, human being, computing device, communication and cloud technologies to support smart applications [1] like industrial control, smart home, health monitoring, smart city, smart grid [2] and etc.. . Here Wireless Sensor Network plays important role to collect the large scale of data from physical phenomenon and send it to the various services [3], and applications running in cloud environment. Senor networks are having the challenges in terms of heterogeneity [4], scalability [5] and energy efficient due to limited processing capacity, bandwidth constraint and energy level. Cluster based techniques in WSN achieves energy efficient by minimizing number of control packets used in network communication. Many techniques are proposed to select Cluster Head and cluster member assignment. The cluster head selections are broadly classified as centralized and distributed. In IoT context distributed approach gives good performance. CM sense the environment and send the information to CH and it forwards to base station in most of the WSN application scenario. Many trust based solutions and access control methods are proposed for secured communication. The objective of secure, energy and band-width aware cluster head selection is not addressed by many of the research work. In general delay energy distance and number of neighbors can be used for cluster election. This work elects cluster head using energy, bandwidth, delay and device trust. The device trust parameter ensures the security constraint among device communication and bandwidth parameter addresses the barrier in heterogeneous network device communication.

Revised Manuscript Received on May 28, 2019.

Thirukkumaran R, kumaran.satinfo@gmail.com, Electronics and Communication Engineering, Saveetha School of Engineering, SIMATS, Chennai, Tamilnadu, India.

Muthu Kannan P, pmkannan@gmail.com, Electrical and Electronics Engineering, Saveetha School of Engineering, SIMATS, Chennai, Tamilnadu, India.

II. RELATED WORKS

Literature study shows that IoT trends to a lot of security threats. This security threat blocks the authorized user performance in the network. Therefore, requirement for different security challenges and its analysis needed in the IoT network. Trust based technique is developed to protect the security threats in the IoT network. This section briefs literature review of existing security techniques used in IoT.

Praveen. et al. [6]., combined the ABC algorithm and GS algorithm for IoT enabled WSN. It takes the distance, delay, energy, temperature parameters of the sensor nodes to select the CH. The evaluation of this algorithm carried in terms of network sustainability and convergence.

Shalli. et al. [7], proposed ME-CBCCP algorithm using minimum energy consumption and chain-based cluster coordinator technique for energy efficient IoT. Network design was introduced based on different communication level like local cluster communication, inter cluster communication and cluster to base station communication in hierarchical manner. The cluster coordinators balance the load of cluster head. The network lifetime and delay performance of the ME-CBCCP were analyzed.

Suyambu. et al. [8], proposed energy aware and secure protocol for WSN routing. At initial stage k-means clustering is used later on based on Link Quality Appraisal (LQA) parameter of nodes grade points are evaluated. By using trust and distrust concept secure path is established. The performance of the proposed system is analyzed in terms of throughput, delay and energy consumption.

Aniji. et al. [9], proposed a dynamic cluster head election method (DCHSM) for IoT applications. The large-scale network area is divided into

small clusters with minimum coverage area by using voronoi diagram. Two levels are used to select the Cluster head in this method. In first level, perceived probability is used and in level two, survival time estimation method is used. The performance analysis shows the improvement in energy savings and network lifetime.

Ming-Yu. et al. [10], presented virtual CH election method (VCHEC) for WSN. By applying Virtual ID concept, it avoids nearby cluster heads and fully covers all cluster nodes. For energy efficient CH election highest residual energy parameter is also considered. The performance analysis carried in terms of number of live nodes, energy consumption and number of cluster head elected.

Fahimeh. et al. [11], proposed TOPSIS based cluster head selection method for wire-less sensor network. It uses four attributes residual energy, number of neighbors, transmission range and distance from base station to select the best node. The performance analysis carried in terms of number of node dies.

III. EXISTING SYSTEM

TAACS-FL [12] is an existing system which focused on trust value computation and cluster head selection. Trust value is computed based on previous behavior of sensor nodes whereas the CH selection is purely depending on highest remaining energy level of corresponding nodes. The parameters like SFR, ECR and DI are used to compute the trust value by applying fuzzy logic. The access right is assigned to each node based on the trust value of corresponding node. In inter cluster routing method every node has to send data packets to its cluster head and the cluster head has to forward those data packets through intermediate cluster head to BS.

IV. PROPOSED SYSTEM

A. *Protocol Design*

Security is an important measure for Internet of Things, due to its dynamic nature and distributed deployment of sensors. The selection of secured cluster head is a primary objective pertaining to secure data communication in cluster based architecture. In TAACS-FL, the highest residual energy contained in the node is the criteria taken for the election of cluster head. Whereas TBCHS-T uses trust value, RBR, and PRD parameters to identify best node and the same is elected as cluster head. Fig.1 shows the block diagram of TBCHS-T.

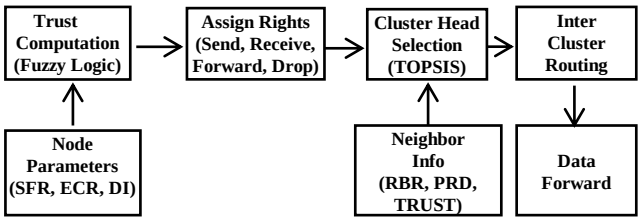

Fig. 1 Block diagram of TBCHS using TOPSIS Method.

The CH has to forward more data than other nodes, so that CH requires more energy and bandwidth. The trust value parameter ensures that the selected cluster head is not a malicious node. Another parameter called PRD ensures that the selected cluster head is closer to the BS.

In TOPSIS the competitor for alternative is the number of neighbor nodes, the selection criteria of alternative is based on attributes like RBR, PRD and trust value of all neighbor nodes. TOPSIS method results hypothesis between two alternatives. One which has the best level for all attributes considered as Positive Ideal alternative and the other one which has the worst attribute values considered as Negative ideal. TOPSIS assigns rank to all neighbor nodes based on the condition that, the distance between the positive ideal solution and how far from negative ideal solution. A node that has got highest rank is selected as a cluster head.

Table 1. Neighbor Table Content

Node	Trust	RBR	Delay (Sec)
node1	0.79832	0.65	0.016289
node2	0.47891	0.81	0.019883
node3	0.21829	0.65	0.009373
node4	0.78935	0.79	0.009236

The values of the chosen parameter for corresponding nodes are stored in a table called neighbor table shown in Table 1. The computed parameter values are shared among neighbor nodes through HELLO message. The selection process of CH is initiated once the network is up and running. In distributed cluster head election process every node compares its own parameter values with all neighbor nodes parameter value. Any node can declare itself as a cluster head if it holds highest rank among all neighbor nodes. The step-by-step instructions are given below.

Step 1: Construction of Decision Matrix The decision matrix (m x n) of TOPSIS is framed using neighbor table values in which number of alternatives (nodes) are considered as m and the numbers of criteria (parameters) are considered as n.

$$Dm = \begin{bmatrix} 0.79832 & 0.65 & 0.016289 \\ 0.47890 & 0.81 & 0.019883 \\ 0.21829 & 0.65 & 0.009373 \\ 0.78935 & 0.79 & 0.009236 \end{bmatrix} \quad (1)$$

Step 2: Derivation of Standardize decision matrix: It is necessary to convert the monotonically decreasing into increasing values. This conversion is computed by subtraction the actual parameter value from the maximum worst value of the corresponding parameter.

Step 3: Construction of normalized decision matrix: Initially the sum of square values of corresponding criteria is calculated for all alternatives in decision matrix. Criteria value of an individual node is divided by the sum of square values of corresponding criteria.

$$nij = \frac{rij}{\sqrt{\sum_{i=1}^{m} rij^2}} \quad (2)$$

Step 4: Construction of

weighted normalized decision matrix: The weight value is assigned to each criterion so that a single dimensional weight matrix is formed. The weight value is decided based on the contribution pertaining to core functionality of chosen parameter. The weighted normalized decision matrix is constructed by multi-plying weight matrix (W) with normalized decision matrix (N).

$$V=NxW \quad (3)$$

The weight value is assigned based on the application requirements.

$$W=\{0.5,0.25,0.25\} \quad (4)$$

Step 5: Computing method for Positive and Negative Ideal Solution:

The positive ideal solution matrix is constructed by subtracting individual nodes criterion value from the highest value of the corresponding criterion value. The negative ideal solution matrix is constructed by subtracting individual nodes criterion value from the worst value of the corresponding criterion value. Positive Ideal solution is computed as,

$$v^{+} =[(\mathrm{Max}(v_{i,j}), j \in j_1),\ (\mathrm{Min}(v_{i,j}), j \in j_2), i=1\ldots m] \quad (5)$$

Negative Ideal solution is computed as

$$v^{-} = [(Min(v_{i,j}), j \in j_1), (Max(v_{i,j}), j \in j_2), i = 1 \ldots m] \quad (6)$$

Step 6: Separation of Measures: This Separation of measures is found by taking square root of the sum of the square of all criterion values in positive and negative ideal matrix. It is understood that this matrix will be [mx1] matrix

Relative distance to the positive ideal solution was calculated as

$$SM_i^{+} = \sqrt{\sum_{j=1}^{m}\left(v_{ij} - v_j^{+}\right)^2} \quad (7)$$

Relative distance to the negative ideal solution was calculated as

$$SM_i^{-} = \sqrt{\sum_{j=1}^{m}\left(v_{ij} - v_j^{-}\right)^2} \quad (8)$$

Step7: Relative Closeness to Ideal Solution:

The relative closeness is calculated as the ratio of the separation measure of negative ideal solution to the sum of separation measure of positive, negative solution in ideal case.

$$CL_i^{*} = \frac{SM_i^{-}}{SM_i^{-}+SM_i^{+}} \quad (9)$$

Step 8: Ranking: The ranking of all neighbor node is assigned based on the value of relative closeness ideal solution. The final rank output is shown in the Table 2.

Node which holds highest rank among all neighbor nodes is declared as Cluster Head. In this example node 6 has the first rank among other nodes in the neighbors so it is selected as cluster head. The election of CH message is sent to all one hop nodes of the CH. All nodes which receive this message will become a member node of corresponding cluster.

Table 2. Rank Output

Node	Rank
22	4
17	2
6	1
31	3

V. PERFORMANCE EVALUATION

The proposed protocol is evaluated for its performance using Network Simulator NS2.

A. *Simulation Parameters*

The simulation parameters which are configured in NS-2 is listed in Table 3. Some of the parameters which are mandatory for WSN are network simulation area, number of nodes, initial energy and simulation time. It also considers packet size, data interval, Tx power and Rx power. The overall simulation area is 500mx500m in which sensor nodes are deployed randomly. The sensor node density varies in the range of 100 nodes to 250 nodes for different scenario. Different types of attacks like data modifier, packet dropper and selfish node are simulated to evaluate TBCHS-T in terms of net-work performance. All sensors have to produce values pertaining to temperature sense application.

B. *Performance Metrics*

Packet Delivery Ratio (PDR): It is computed by dividing number of data packets received at BS with number of data packets sent by all sensors.

Throughput: It is defined as the number of data bits received per second (bits/sec) at BS.

Average Energy Consumption (AEC): It is the ratio of net energy consumed by all sensors in the network to the total number of sensors.

Average End-to-End Delay: The delay value of each packet is calculated by subtracting packet sent time at sensor from the packet receive time at BS. The sum of delay values of all packets received at BS is calculated and divided by total number of data packets received at BS, and it called as Average End-to-End delay.

Control Overhead: It is calculated by the number of control messages used to achieve reliable and secure data transmission. These control message packets are used to share the information about updates in routing table, cluster selection and inter cluster communication.

Normalized Routing Load (NRL): It is the ratio between number of control messages used to the number of data packets received at BS.

Table 3. Network Simulation Parameters

Parameter	Value
Network Simulation Area (m)	500 x 500
Total Number of nodes	100 to 250
Total Simulation Time (s)	1000
Initial Energy (J)	100
Tx Power (mW)	0.6
Rx Power (mW)	0.3
Number of Attackers	3 to 15
Data Packet Size (bytes)	64

Data Transfer Interval (s)	0.1

C. *Varying Number of Attackers*

In this scenario all parameters used for the simulation is kept static except the attackers. The number of attackers is gradually increased from 3 to 15. As mentioned earlier the types of attacks simulated here are packet dropper, selfish behavior and data modifier, which is used to evaluate the performance of TBCHS-T. Total simulation time used is 1000s and the sample result values are produced 10 times with different scenarios and average sample result values are plotted.

The CH is selected purely depends on the highest residual energy of the sensor node in TAACS-FL. The parameters like RBR, PRD and Trust value are considered in the selection process of CH in TBCHS-T which results an improvement in evaluated network performance parameters.

Packet delivery ratio is usually high in a secured data communication. Fig.2 illustrates that TBCHS-T has got better packet delivery ratio comparatively TAACS-FL. This implies that the implemented protocol is able to isolate malicious node and successfully forward data packets to the corresponding BS. The CH selection is another important criteria. The trust value and the residual bandwidth ratio (RBR) are used as criteria for selecting CH. A node which holds highest free bandwidth and more trust value is selected as a CH which ensures highest packet delivery ratio and secure data communication. The implemented protocol is able to achieve reason-ably good PDR even the number of attackers is increased gradually.

Fig.3 shows that the average end-to-end delay is comparatively decreased in TBCHS-T. It is evident that a reliable and secured data communication achieved by implemented protocol is a reason for lesser delay.

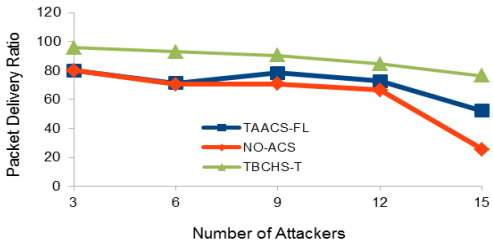

Fig 2. Number of Attackers vs PDR

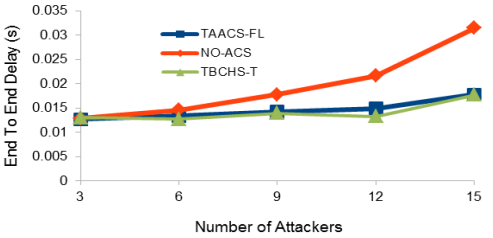

Fig 3. Number of Attackers vs End-To-End Delay

D. *Varying Node Density*

In this setup, the nodes are gradually increased whereas all other parameters used for the simulation is kept static. The total number attackers are 6 and the number nodes vary from 100 to 250. Total simulation time is 1000s and the sample result values are produced 10 times with different scenarios and average sample result values are plotted. The very purpose of this scenario is to evaluate the scalability of the protocol TBCHS-T.

Fig.4 is plotted for the scenario where the number of nodes is increased gradually and number of attackers is kept constant. The implemented protocol is able to achieve comparatively better packet delivery ratio even the network is dense which ensures the scalability of the protocol.

Fig.5 is evident that the implemented protocol is able to achieve good throughput for increased number of nodes. In dense network increased number of nodes will create contention which usually impacts the bandwidth. Even in this scenario the throughput value is reasonably high in TBCHS-T.

The Average energy consumption of the sensor node is lesser in TBCHS-T this shown in Fig 6. This in turn increases the network lifetime even in the scenario of increase number of nodes.

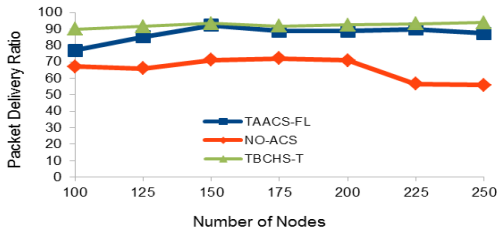

Fig 4. Node Density vs PDR

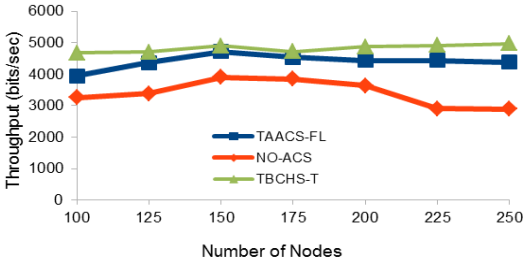

Fig 5. Node Density vs Throughput

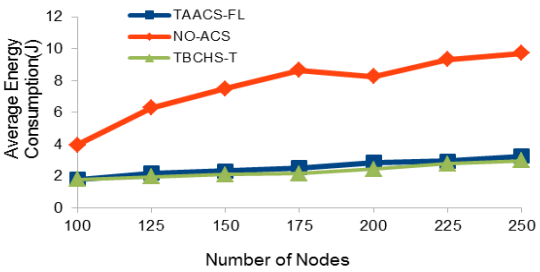

Fig 6. Node Density vs AEC(J)

VI. CONCLUSION

Trust based cluster head selection system using TOPSIS (TBCHS-T) addresses the security issue which is mandatory for internet of things because of its heterogeneous nature and distributed deployment of sensors. In this work the

trust value is calculated using fuzzy logic and the selection of cluster head is executed using TOPSIS method that is nothing but multi criteria decision making algorithm. The parameter selection is focused on heterogeneous network environment and secured data transmission. The simulated results shows reasonably good improvements in all network performance like throughput and packet delivery ratio when it is compared with existing protocol called TAACS-FL. Further the implemented protocol ensures the scalability, increase in network lifetime and security in data transmission.

REFERENCES

1. J. Gubbi, R. Buyya, S. Marusic and M. Palaniswami, "Internet of Things (IoT): A vision, architectural elements, and future directions" in Future Generation Computer Systems, pp. 1645–1660, 2013.
2. V.C. Gungor, D. Sahin, T. Kocak, S. Ergut, C. Buccella, C. Cecati, G.P. Hancke, "Smart Grid Technologies: Communication Technologies and Standards" in IEEE Transactions on Industrial Informatics, pp.529, 2011.
3. T. Park, N. Abuzainab and W. Saad, "Learning How to Communicate with the Internet of Things: Finite Resources and Heterogeneity", in IEEE Access, pp. 1–1, 2016.
4. M. Trnka and T. Cerny , "Identity Management of Devices in Internet of Things Environment", in 6th International Conference on IT Convergence and Security (ICITCS), pp. 1–4, IEEE,2016
5. J. Petajajarvi, K. Mikhaylov, M. Pettisalo, J. Janhunen, J. Linatti, "Performance of a low-power wide-area network based on LoRa Doppler robustness, scalability, and coverage technology", in International Journal of Distributed Sensor Networks, vol.13(3), 2017.
6. M. P. K. Reddy and M. R. Babu, "Energy Efficient Cluster Head Selec-tion for Internet of Things" in New Review of Information Networking, issue 22, vol. 1, pp. 54-70 , 2017.
7. S. Rani, R. Talwar, J. Malhotra, S. H. Ahmed , M. Sarkar and H. Song, "A Novel Scheme for an Energy Efficient Internet of Things Based on Wireless Sensor Network" in Sensors, vol. 15, pp. 28603-28626, doi:10.3390/s151128603,2015
8. S. Karthick, "TDP: A Novel Secure and Energy Aware Routing Protocol for Wire-less Sensor Networks. In: International Journal of Intelligent Engineering and Systems", vol.11, No.2, DOI: 10.22266/ijies2018.0430.09, 2018.
9. A.John, A. Rajput and V. Babu, "Dynamic Cluster Head Selection in Wireless Sensor Network for Internet of Things Applications", In Proceedings of IEEE International Conference on Innovations in Electrical, Electronics, Instrumentation and Media Technology ICIEEIMT- 17,2017.
10. T. Ming-Yu and Y-C Chen, "A Virtual Cluster Head Election Scheme for Energy-Efficient Routing in Wireless Sensor Networks", in 3rd International Conference on Future Internet of Things and Cloud, 2015.
11. F. Hamzeloei and M. K. Dermany, "A TOPSIS Based Cluster Head Se-lection for Wireless Sensor Network" in Procedia Computer Science, vol. 98, 2016, pp. 8-15.
12. R. Thirukkumaran and P. Muthukannan, "TAACS-FL: trust aware access control system us-ing fuzzy logic for internet of things", in Int. J. Internet Technology and Secured Transactions (In press)

AUTHORS PROFILE

Thirukkumaran R has completed his B.E, in Electronics and Communication Engineering in Kongu Engineering College in 1995. He has completed his M.E. in Communication Systems in Karpagam college of Engineering affiliated to Anna University in 2012. He is currently a research scholar in Saveetha Institute of Medical and Technical Sciences, Chennai. His research interests are Internet of Things, Network Security, Wireless Networks and Sensor Networks.

Dr Muthu Kannan P completed his Bachelor and master's degrees in engineering in 1993 and 2000 respectively. He was awarded doctorate in 2012. He is currently serving as Associate Dean - Examinations in Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai. He has 25 years of teaching experience. He has published 25 papers in Peer reviewed journals and 25 papers in International and National conferences. His research interests are Antennas, Wireless Networks and Image Processing

.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication