Journal of Information Technology Management

Print ISSN: 2008-5893

Online ISSN: 2423-5059

Cluster Node Migration Oriented Holistic Trust Management Protocol for Ubiquitous and Pervasive IoT Network

Anup Patnaik

*Corresponding Author, Research Scholar, Department of Computer Science and Engineering, Centurion University of Technology and Management, Odisha, India. E-mail: patnaik.a@hotmail.com

Banitamani Mallik

School of Applied Sciences, Centurion University of Technology and Management, Odisha, India. E-mail: banita.mallik@cutm.ac.in

M. Vamsi Krishna

Department of Computer Science and Engineering, Chaitanya College of science and Technology, Madhapatnam, Kakinada, India. E-mail: vkmangalampalli@gmail.com

Abstract

Smart applications with interconnected intelligent devices for sharing services arise serious security problems to the stability of this IoT complex and heterogeneous environment. Unless security considerations are analyzed and implemented properly in real time then IoT cannot be perceived as a pervasive network for the possible stakeholders. Current state of the art has analyzed trust-based security solutions as additional feature to application layer of the system which can identify and filter out the malicious nodes. In this paper we are proposing holistic trust management with edge computing mechanism to create trustworthy zones comprising different clusters, where Gateway on behalf of clusters will initiate migration of their nodes if falls below the defined Zone trust threshold level. The created zones are self-resilient against any malicious attacks and saves lots processing usage time and energy to address the security issues. By analyzing our proposed algorithm with other contemporary approaches to handle IoT security issues using trust mechanism, this approach is more precise in terms of protecting system against incurring malicious behavior, and also prolong the application operation duration by reducing communication and processing overhead.

Keywords: Internet of Things, Heterogeneous environment, Clustering, Oriented Holistic trust management.

DOI: 10.22059/jitm.2021.80027

Introduction

IoT, a new paradigm in networking world shifted the industries and researcher's focus from wireless sensor network to more complex and heterogeneous environment, involves different components such as smart devices, gateways, clouds, predictive/prescriptive analytics and then finally, application reports. Currently millions of devices are interconnected to provide customer-oriented services to ease the human life, for this purpose there are different domains where the contributions of IoT are very significant to influence decision making system, reduces the manual intervention to monitor the application objectives, therefore providing Intelligent solutions to the real time application through smart devices is the main vision of this network. Additionally, smart devices operate on different environmental and application factors which decide type of connectivity needed at this stage to achieve the goals. Mostly the widely used device-oriented communication protocols for connectivity are Wi-Fi, Bluetooth, ZigBee and 6LoWPAN suitable for short range IoT physical elements like sensors, actuators, and small computing systems and gateway or end devices, but in some cases, these devices' boards are embedded with multiple communications protocols provision.

Table 1. IoT Communication Protocols

Wireless IOT Connectivity	
Short Range Protocols	**Long Range Protocols**
Wi-Fi	Cellular
Bluetooth	2G(GSM)
6LoWPAN	3G(GSM/CDMA)
Z-wave	4G(LTE)
ZigBee	5G(Available 2020)
ANTIANT	LTE Cat 0,1 & 3
Thread	LTE M1
NFC	LTE NB1
RFID	NB IOT
EnOcean	LPWAN
	LoRaWAN
	Weightless N
	SigFox
	Ingenu
	Neul
	N Wave

These protocols as mentioned in Table 1 vary from each other, based on frequency, range, and data transmission rate parameters and the edge computing translates this communication protocols instruction to internet protocols to send the collected data to the cloud. There are many virtual or physical components started mapping from things layer to People and Process Layer, builds the type of application levels required for the scenario, it could be simple or complex level from level 1 to level 6 where each level contains distinct local and cloud components (Table 2). Mainly, the devices used in WSN (Wireless Sensor Network) aims to collect unformatted data from environment interaction, also need to aggregate the collected data and send to the nearest station. Devices with different types of data, memory capacity, processing capability, transmission range and communication protocols make these contrasting to its properties to the data link layer. Current IoT challenges are quite serious to adopt in real time, in addition to win the trust of different components which are facilitating the application functions either local or cloud level to system makes it more vulnerable.

In the literature review on existing approaches, survey on new prototypes and research on security mechanism, the summary is trust mechanism, which is the alternative solution to build the security gaps and provides the flexibility to nodes to communicate under uncertain circumstances. Such situations further deteriorate with more troublesome when nodes are involved in delivering fake recommendation to promote/demote nodes to alter trust value to influence the interactions. This fake recommendation initiates different type of attacks inside trust-based system.

- Good Mouthing Attacks: Provides good recommendation to fake objects to promote its trust value
- Bad Mouthing Attacks: Provides bad recommendation to good objects to demote its trust value
- Self-Promoting attacks: Provides good recommendation to itself to promote its trust value
- Selective forwarding attacks: Only forwards selected packets and drops other packets
- Sinkhole attack: creates the fake information and sends the route request to neighbor nodes

Based on the previous research motivation in forming clusters in the network, our proposed approach here is extending the cluster to trustworthy zones formation, i.e. group of clusters entails to the concept of node migration with help of cluster heads under supervision of gateways. Average trust value level of cluster head is compared individual nodes trust level

and the node's level falls below average value of CH, then node is pushed to the CH migration list, therefore segregation of nodes inside clusters could be achieved through the trust evaluation process. Node migration is not possible if there are no other clusters to accept it or not having enough energy to move to the other cluster. In case, no node migration cases, the cluster head will exclude such nodes from interaction for specific duration/period of operational time, further these excluded nodes can be included back and stays within their cluster zone after their connection request initiation acknowledged by cluster head. Instead exclude from interaction, cluster head also drops the nodes permanently if these are nodes fall below average trust threshold level and also its remaining energy less than the cut off level, therefore these nodes are marked as malicious, immediately updated their reputation value and prevented these nodes in any means involved in trustworthy operations. Every cluster head can advertise its external requirements and send it to neighbor cluster heads which may accept or reject it. As per our current knowledge base, it is kind of first time that our proposed approach initiates share one CH trusted nodes to other CHs to accomplish its purposes.

Table 2. IoT System Components

IoT Component	Component Roles	IoT Layer
Resources	Software components plays crucial role connect to network, communicate datalink protocols, access & store the data and controlling actuators	Things Layer
Controller Services	Runs on device and communicates with webs service to handle application commands	Connectivity/Edge Computing Layer
Local/Could Database	Stores Data generated by Devices and application logs	Data Ingestion Layer
Web Services	Bridges between application and device, also reaches to database to store through end points	Global Infrastructure Layer
Analytics/Artificial Intelligence	Analysing the massive device data stored in cloud and draws inferences for decision system	Data Analysis Layer
Web Application/Mobile app	Gather data based on the requirement and monitor the collected data, pushes the data for further analysis	Application Layer
Business Reports	Reports are generated based on previous step analysis and shared with customers. It can be stored either local or cloud platforms.	People and Process Layer

Finally, the remaining of this paper is structured as follows; Section 2 presents current state of art related to trust management and security issues in IoT network. Discussion on our proposed protocol is outlined in Section 3 and provides new direction creating trustworthy zones to avoid malicious attacks of nodes. Section 4 presents the results achieved in the simulation considering different network impacted parameters then followed by our current research work conclusion and, the direction of future works cited as well.

Literature review

Shah et al. (2015) proposed fuzzy logic controller to achieve expected network lifetime at cost of real time communication and energy consumption. Basically, it controls each node's energy consumption and guarantees it should be optimal to reach the objective. It maintains balanced energy among the nodes by selecting active nodes in each round and use sleep schedule in an efficient way. In each stage fuzzy controller selects active nodes based on remaining energy and active time; also expand the transmission power to reduce number of hops between source and destination. The general semantic based trust mechanism in Wang et al. (2013) involves extracting trust information, calculating the trust value, sharing calculated information and finally decision making for self-organizing set of nodes which going to stay for providing the service to service requester. In extracting trust information, it will extract trust information from each layer sensor, core and application layers, so overall trust value is calculated by the weighted sum of each element with giving different importance of each layer and users preference.

The application layer security provided by Abhijit and Prasad (2018) is trust model for IoT and fog ecosystem. Trust based data communication along with other security approaches are employed to filter out security attacks. There are four layers in this IoT and fog system where trust-based security is implemented at fog layer that communicates only authenticated data to the cloud. Authentication, access control, and light weight cryptography algorithms are used to setup initial IoT network and fog nodes before actual data transmission starts.

Designed framework by Fernandez-Gago et al. (2017) considered interoperability, dynamicity and fragmented research to address IoT challenges related to trust, privacy, and security. Framework having tools and services are providing benefits to the end users of IoT which includes the trust concerns. This framework advocates the trust calculation at run time helpful to leverage the reconfiguration in self adaptive system. Its four-layer architecture where trust framework layer includes package of services can be used in different context of system, exposed as API for designers and developers, further it can be extended through its base components, public methods and configuration files.

Trustworthiness of device in Tragos et al. (2016) calculated based on different criteria such as communication-based trust, Security-based Trust, Data-Reliability based Trust, Social Relationship based Trust, and Reputation based Trust. The Trust value obtained through different approaches can be used as IoT services for data sharing, access control, authorization, indoor positioning solution, and routing. Further, IoT domain includes many scenarios which can use the trust prominently for the exchanging information from users to devices, for actuating commands from device to user and for information and commands between devices. Design of trust model aiming to find malicious activities/malfunctioning

nodes considers the following steps observation, scoring, selection, transaction reward and punishes to be incorporated.

The selection of cluster head is to balance the load in the network and also, helps to reduce the energy consumption and increase the lifetime of networks. This algorithm in Behera et al. (2019) considers initial energy, residual energy and optimal value of CH to be elected cluster head for the next level of operation. R-LEACH model adopted in this approach shows better network performance in terms of more packets delivery to Base Station (BS), of network, throughput, reduce latency, optimal use of residual energy.

Oumaima Ben Abderrahim et al. (2016) provided security solution through trust management clustering algorithm to protect the network from malicious attacks most likely caused by cluster head and also improved the network lifetime. It considers parameters such as trust level, energy, connectivity, stability and Community Interest to select the cluster head. Since IoT having heterogeneous and anonymous, hence clustering algorithm is based on the context and stability. Same context is required as it helps high level of interactions among the devices for having common settings and grouping of objects happening based on their locations to prevent loss connection and in memory data frequently.

Alshehri et al. (2018) focused on scalability of trust solution to billions of IoT nodes which addresses trust-based clustering, counter trust related attacks, trust value computation and trust migration. This proposed IoT-TM includes four algorithms part of IoT trust management includes filtering bad mouthing of trust values, determines the node to join the cluster, cluster formation, and finally migration of nodes. The simulation shows evenly distributed nodes based on their trust value creates smaller difference in average trust values among the master nodes.

Layer architecture used in Dedeoglu et al. (2019) for improving end to end trust from data observation to block validation in block chained based IoT applications. This approach initiates the trust validation at data link and block chained layers separately, in data link layer it considers evidence, reputation of source and confidence on its collected data and in BC layer inter node interactions termed as transactions are evaluated through the customized block chain architecture with the following steps block generation, block validation, and distributed consensus mechanism.

The trust architecture for soft defined network (SDN) in IoT called IoT trust integrated with cross layer authorization protocol Chen et al. (2019). Further, trust evaluations methods depend behavior-based reputation evaluation scheme for the Node and an organization reputation evaluation scheme for organization, both together decides whether node will get access of the tag or not. Cross layer authorization protocol authorizes the node to access to the tag related organization based on the node and organization's reputation. With the gain of

popularity of IoT in real time scenario connected with multiple heterogeneous devices, Mohan and Bhanu (2018) sensed the challenges inherent inside IoT life early and proposed the multi-dimensional trust aware routing framework considering social trust (direct and indirect trust) and also information trust to select next hop node. The other network parameters, for increased network lifetime and less average energy consumption, this framework adopted clustered strategy and all the communication responsibilities are allocated to the cluster heads. This approach is effective in securing the IoT network against the attacks proved through the simulation by varying from malicious rates.

Meng et al. (2017) proposed new intrusion detection systems (IDSs) to safeguard against inside attacks using trust management mechanism. Packet based trust management mechanism may not be effective in case of heavy traffic, therefore Bayesian-based trust management is used in this model. From the above literature survey, it is quite evident that none of the above approaches firmly addressed the issues of cyber-attacks, scalability, and energy utilization of nodes in IoT. Today's generation IoT applications demand high accuracy of privacy/security protection against mischievous nodes and to give trust and confident to the user to participate in IoT uncertainty world.

Maddar et al. (2018) has presented the effective model of distributed trust management approach in the application of IoT. This approach evaluates the human interaction of 1000 to 5000 datasets. Here, various components in IoTs selected from the object, which performs the dynamic characteristic based real world applications. Security model of WSN performed with internet based applications. Intrusion detection on WSN performs the various attack reduction by functions used in network model. The internet attack represented as manufacturing attack, selective forwarding attack, Sinkhole attack, Black hole attack and jamming attack. This review analysis the various attack detection models to get the better algorithm.

Pourghebleh & Hayyolalam (2019) has presented the review analysis of systematic approach of load balancing in IoT application. The utility of IoT application single system performance leads the network overhead problem; so, the optimized IoT designed to reduce the imbalance traffic analysis. Centralized and distributed approach on load balancing scheme utilized to get the result of scalability, routing, reliability and security. Krishna, (2017) has designed the security management approach of IoT with RFID network analyzer. Here, it utilizes the Web of Thins with heterogeneous systems. This adopts the communication technology on wireless network, which utilize the cyber physical network for different approaches in IoT. Trust management, delay, network overhead, security and reliability parameters are determined to obtain the better security based trust management protocol.

Table 3. Trust model comparisons

Trust model category	Trust model	Approach			Trust computation technique	Performance
		Centralized	Distributed	Blockchain Based		
Cross-layer authorization trust model	Chen et al., (2019)		✓		BES and ORES trust evaluation	Enabling the reliable data collection/mining, context-awareness, and enhanced user security in the IoT
Layered Trust model	Wang et al., (2013)		✓		Fuzzy set and semantic mining approach	Decision making, self-organization, service components and trust solutions
Data oriented trust model	Tragos et al., (2016)	✓			Fuzzy logic or data fusion techniques and cryptography for security	Data sharing approach with secure model. Communication, security, data-based criteria, social relationships, and reputation.
Data oriented trust model	Maddar et al., (2018)		✓		Location Detection Using the TDOA geo-location Algorithm	Network attack detection
Data/packet oriented trust model	Oumaima Ben Abderrahim et al., (2016)	✓			Intergroup topology, Threshold based trust model	Network lifetime and network attack detection
Blockchain based trust model	Dedeoglu et al. (2019)			✓	Data trust and gateway reputation model	End to end trust from sensor data observation to blockchain validation
Scalable trust model	Alshehri et al. (2018)	✓			Trust Management scalability trust algorithms	Scalable trust management prevents bad mouthing attacks

Different models of blockchain also enhance the security, transparency and trust among various actors in supply chain management. In Khanna et al. (2020), permissioned blockchains can be used in many supply chain management ecosystems. This research prototype can be extended to IoT applications to establish trust between unknown devices for shared services. In wireless sensor network (WSN), there are approaches to find the attackers to trace their ability to clone good nodes parameters but Juneja et al. (2017)'s witness based distributed mechanism is able to detect the clone attacks with high detection probability and less memory overhead compared to other algorithms. Currently it works only for static WSN, can be extended to WSN along with considering mobility of nodes. Juneja et al. (2020), evaluated seven parameters from the identified 11 wireless communication technology by using multi-criteria decision making approach and ranking was obtained to choose right

platform for industry 4.0 applications. Table 3 summarizes comparison points between these different trust-based mechanisms followed for IoT applications.

Proposed model

Concept of edge computing in our proposed model that plays vital role in formation trustworthy zones, i.e. enhancement of single cluster to multiple clusters joining to form trustworthy zones. Main intent of our approach to form trustworthy zones across network and the lead node of CHs will do the direct interaction with base stations. This approach is very much flexible than other current algorithms because it could be used for both single and multi-hop communication to base station. Most of the algorithms in current state of art facilitate either single or multiple hops communication but here in our approach can stand by both based on the application requirement. Core notion of forming trustworthy zones through cluster chaining mechanism is of unique approach as per our survey and helped IoT network world to resolve many inherent issues, which lasted for long time.

Further, this model is considering different network parameters to select cluster head, than other primitive models where it considers one or two parameters which may not be suitable to judge the head among the nodes. In such situation always high chances are there for selected head node might be wrong one who dissipates the energy quickly, then impacts whole network functionality adversely. After gateway calculates every node trust value based on the below equation (1), it decides the node with highest as head and second highest stays as clone to head to support main head during the execution cycle. First CH and second clone head together share their own cluster load and controls node communication, node migration, node connect/disconnect. Most likely clone cluster head, the second highest trust vale will replace actual cluster head in future. After completion of operation in interval t1, the next interval t2 clone cluster head will act as cluster head till gateway finds another new cluster head. Using this notion, not only it saves execution time for service operations, energy to collect and transmit the data, reduces communication messages, more important its independent of finding new cluster head on the next interval.

Cluster Head Selection based on the below equation

$$Trust\_Val_{Node} = Energy\_Residual_{Node} + Energy\_Transmitting_{Node} + Reputation\_Value_{Node} + Density_{Node} + Communication\_Range_{Node} \quad (1)$$

- Trust_Val$_{Node}$: Trust value of a node present inside a cluster, range from -1 to 1, where 1 stand for very honest and -1 stands for dishonest node

- Energy_ Residual Node: Remaining energy of node which will be used for future transactions

- Energy_ Transmitting $_{Node}$: How much energy is consumed by node to transmit k bits of data from its cluster to other cluster. If node involves any kind malicious activities inside network, definitely it has to spend more energy than expected.

- Reputation _Value $_{Node}$: Service provider sends request to neighboring nodes to get the reputation of service requester, which involves the past interactions of service requester to different nodes. In our proposed model, we only consider latest and long-time duration interactions of the past interaction of node, but other algorithms consider all interactions irrespective of execution time and duration.

- Density$_{Node}$: Service requester, how well placed in network is very crucial to consider its request, based on its network density node can ensure less energy depletion and increase network lifetime.

- Communication _ Range$_{Node}$: This is specific to device communication protocol, service provider can decide before initiating transaction whether requester node's communication range is apt to grant the approval of its request.

Nodes in the cluster can map to either CH or CLCH sharing its unique identity, data in both heads are combined represents total number of nodes present in the cluster. After the selection of cluster head, the next task is to find trust of nodes inside cluster. Our approach considering direct, prioritized reputation values and other network parameters find the trust value of node. CH and CLCH defines the trust value range to perform based on gateway decision. Multiple cluster heads architecture as in is followed inside our cluster to balance the cluster workload and not to overburden the single CH, as implemented in other models. Mainly main cluster head will respond to the instructions given from gateway and updates the status later to it. The other cluster head will facilitate the transfer the sensors collected data to the upstream IoT levels. The whole mechanism is classified as gateway mapped to CH and sensors/transducers mapped to CLCH, finally CH and CLCH will interact with each other to share the tasks and maintain the cluster balanced in terms of residual energy, turn-around time, and memory usage.

Average trust value level of cluster head (CH) and clone cluster head (CLCH) is compared to individual nodes trust level and the node's level falls below average value of CH, then node is pushed to the CH migration list, therefore segregation of nodes inside clusters

could be achieved through the trust evaluation process. Node migration is not possible if there are no other clusters to accept it or not having enough energy to move to the other cluster. In case, no node migration cases, the cluster head will exclude such nodes from interaction for specific duration/period of operational time, further these excluded nodes can be included back and stays within their cluster zone after their connection request initiation acknowledged by cluster head. Instead exclude from interaction, cluster head also drops the nodes permanently if these are nodes fall below average trust threshold level and also its remaining energy less than the cut off level, therefore these nodes are marked as malicious, immediately updated their reputation value and prevented these nodes in any means involved in trustworthy operations. Every cluster head can advertise its external requirements and send it to neighbor cluster heads which may accept or reject it. As per our current knowledge base, it is kind of first time that our proposed approach initiates share one CH trusted nodes to other CHs to fulfill its purposes. Trustworthy zones and multi CH on IoT network is shown in Figure 1.

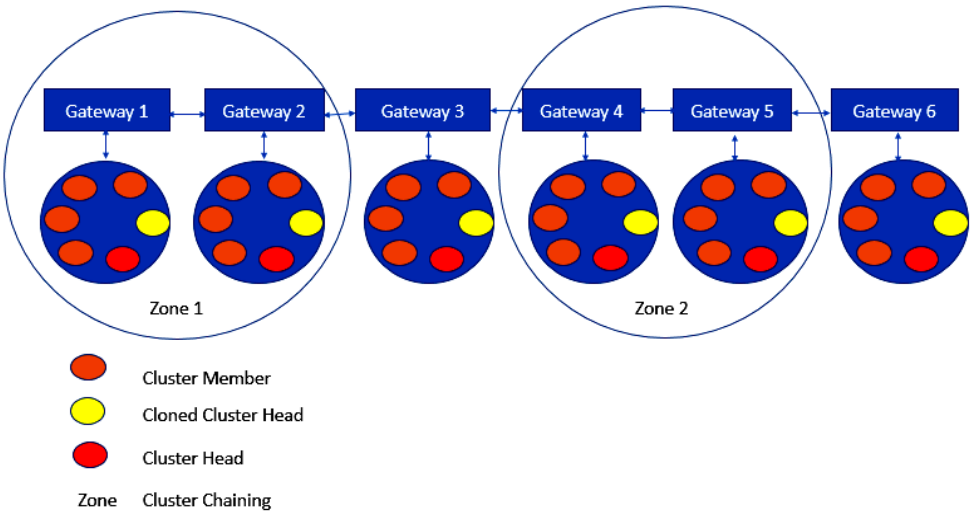

Figure 1. Trustworthy Zones and Multi cluster head architecture of IoT network

Algorithm

Input: Random IoT Network with different capabilities devices with fixed range of communication

Step-1: Random Network is transformed to different clusters by gateway using above modified LEACH (Low-energy adaptive clustering hierarchy) clustering model and cluster density will remain same among the clusters.

Step-2: Edge computing in the network makes different clusters and finds out the CH and CLCH in every cluster. These two nodes are the highest trust level among all the nodes in the cluster.

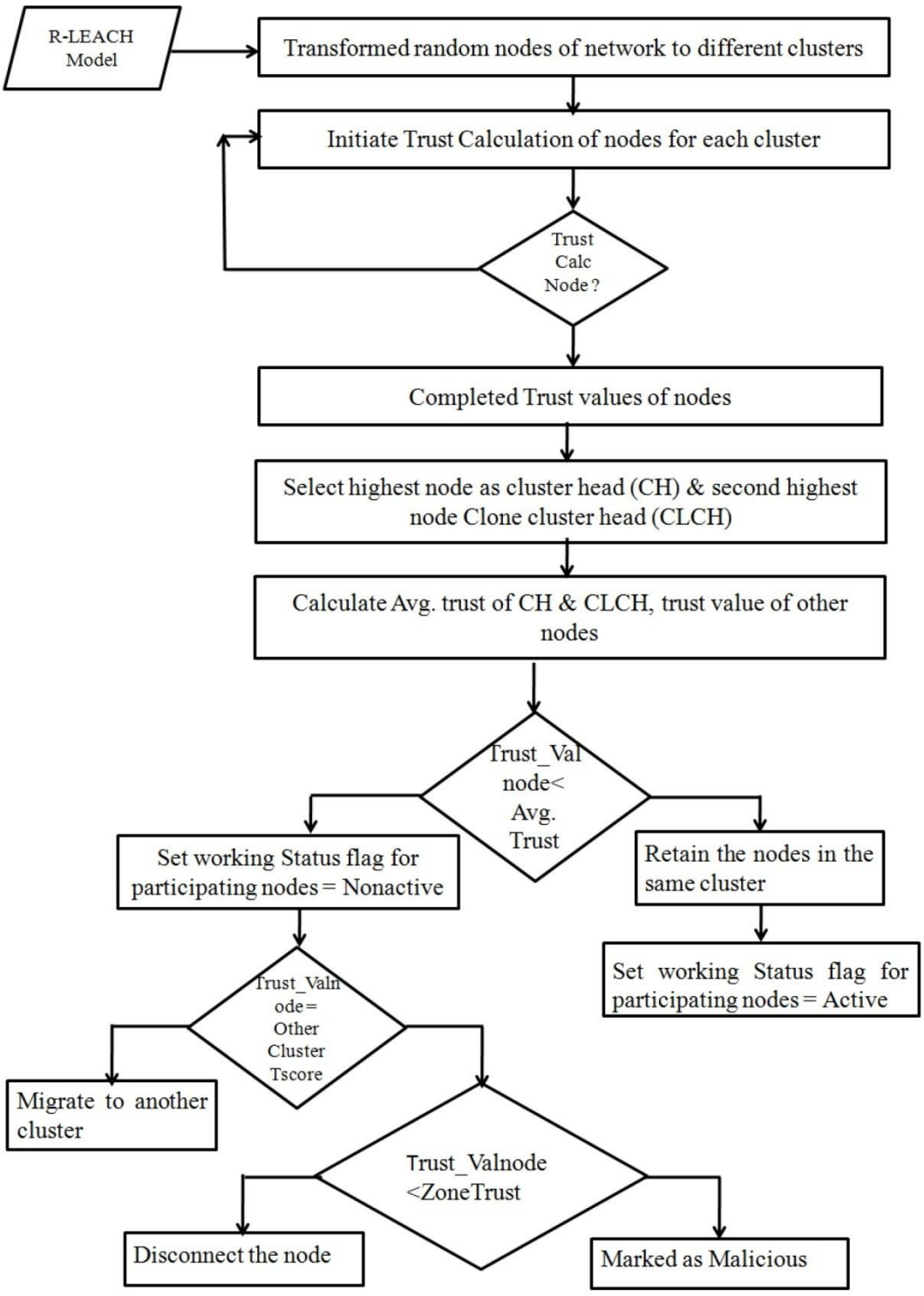

Figure 2. Proposed Trust Model flow

Step-3: CH will interpret the instructions from gateway and pass either to CN or CLCH based on criticality of task. CLCH will keep on supporting & monitoring the sensor nodes.

Step-4: After formation of clusters, next task of edge computing of gateway is to create trustworthy zones which maps multiple clusters into one zone based on similar application context.

Step-5: Every cluster is managed by CH and CLCH, CLCH makes nodes temporary disconnect if not participating active operations which saves energy. Finally, data stored in both cluster heads are transferred to base station.

Step-6: Trust of node falls below average trust of CH & CLCH, then node is ready for migration to other clusters or gateway depending on other cluster's trust score and Zone trust score, temporary off from active transactions and also, all other nodes stop interacting with this specific node after confirmation received from CH.

Step-7: Calculate average trust score of Zone by Gateway node and sends the score to CH of each cluster.

Step-8: if trust score of a node falls into range of average trust score of other clusters then CH will advertise its node details to other cluster for migration, else if trust score of a node falls below the zone trust score then CH informs the gateway node and marks it malicious.

Step-9: After migration of node, deleted all its reference from previous cluster and mapped to new cluster. Any Node in cluster updated with ready for migration to gateway node then it's marked as malicious node.

Output: With this approach not only, it expedited the turnaround time of sensor service-oriented transactions and, managed to have balanced network in terms of residual energy, turn-around time, and memory usage. It could prevent many trust related attacks and maintained higher level of security and privacy of user data inside network. Proposed trust model flow is explained in steps of Figure 2.

Pseudocode: Finding the active participating nodes and remove malicious nodes

Input: Number of Nodes N_1, N_2, N_n present in random network

Output: Finding active participating nodes and remove malicious nodes

1. Gateway node applies R-LEACH model to network nodes to form clusters
2. If Node belongs to cluster then
3. send acknowledgement to gateway
4. else
5. continue with subroutine of cluster forming
6. end if
7. For I =1 to n clusters

8. Calculate trust of each nodes $Trust\_Val_{Node}$
9. Find the first highest and second highest trust score nodes
10. Set CH = first highest trust score and CLCH = second highest trust score
11. $Cluster_{AvgTrustscore} = (CH_{TrustScore} + CLCH_{TrustScore})/2$
12. If $Trust\_Val_{Node}$< ClusterAvgTrustscore
13. working Status= Not Active
14. Else
15. Working Status= Active
16. $ArrNodes_{CusterIndex}$ = Find the Nodes with NonActive status
17. For I= 1 to Len ($ArrNodes_{CusterIndex}$)
18. If $ArrNodes_{CusterIndex}[i]$ = Other $Cluster_{TustScore\ AND}$ $ArrNodes_{CusterIndex}[i]$
19. then migrate the node to that cluster
20. else if working Status = Malicious
21. END For
22. END For

Performance evaluation

Simulation Model and Parameters

The proposed method simulated with Network Simulator tool (NS 2.34). In the simulation, 100 wireless nodes are placed in a 60 × 60 meter square region for 30 milliseconds simulation time. Each Mobile node goes random manner among the network in various speed.

Table 4. Simulation Setup

No. of Nodes	100
Area Size	60x60
Mac	802.11g
Radio Range	250m
Simulation Time	30ms
Traffic Source	CBR
Packet Size	512 bytes
Mobility Model	Random Way Point
Protocol	AODV

All nodes have the similar transmission range of 250 meters. CBR provides a constant speed of packet transmission in network to limit the traffic rate. AODV routing protocol is applied to obtain energy saving enrichment routing path in the network. Table 4 shows simulation setup is estimation.

Results and Discussion

Evaluation of proposed holistic trust model

X graph in ns2.34 is used for analyzing the simulation performance.

Throughput: successful reception of packets at the receiver is measured and framed with the graph model. The throughput is graphed with the Figure 3 and it shows the improved result of proposed holistic trust model. In proposed holistic trust model throughput is increased as compared to existing scheme Chen et al. (2019).

$$\boldsymbol{Throughput = (Number\ of\ packet\ received/Sent) * speed}$$

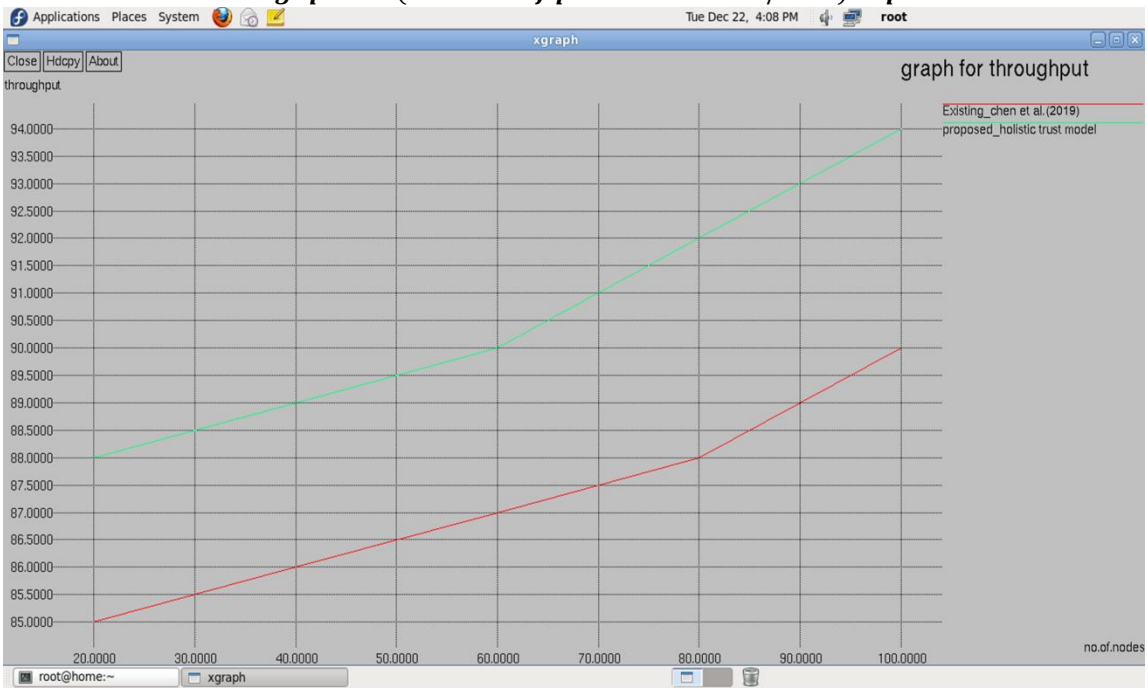

Figure 3. Throughput (throughput vs. no. of nodes)

Network Lifetime: Figure 4 illustrates with speed and transmission rate determined with calculated result of throughput. The network lifetime is improved the overall performance by our holistic trust model. In this, proposed method is used to offering the efficient routing path and the lifetime is increased as compared to existing scheme Chen et al. (2019).

Cluster head overhead: In Figure 5 Cluster overhead is minimized and is also able to filter out the malicious nodes and disconnect the nodes temporarily and it also saves more energy of overall network. In proposed method overhead is decreased as compared to existing scheme Chen et al. (2019).

$$Network\ Lifetime\ =\ time\ taken\ to\ utilize\ network/overall\ ability$$

Figure 4. Network Lifetime (network lifetime (%) vs. no. of nodes)

$$clusterhead\ overhead\ =\ (Number\ of\ Packet\ Losses/Received) * 100$$

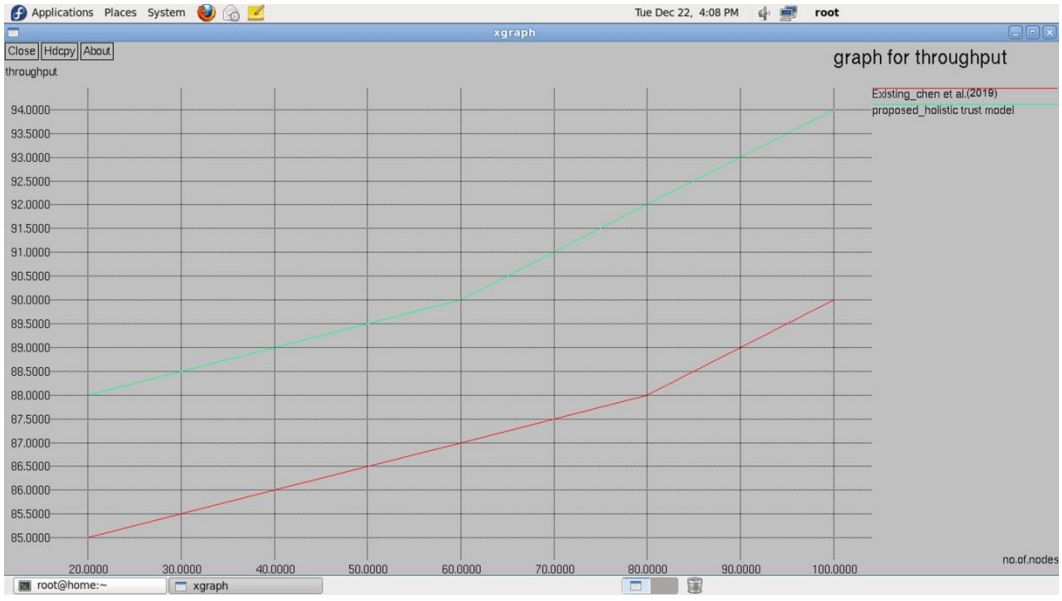

Figure 5. Cluster Overhead (cluster overhead vs. time (sec))

Trust level: In Figure 6, trust level improves with time because it is able to keep only non malicious node in the network prior starting the transaction. Clusters will initiate migration of their nodes if falls below the defined Zone trust threshold level. The created zone is self-resilient against any malicious attacks and saves a lot processing usage time and energy to address the security issues. In this proposed method trust level is increased as compared to existing scheme Chen et al. (2019).

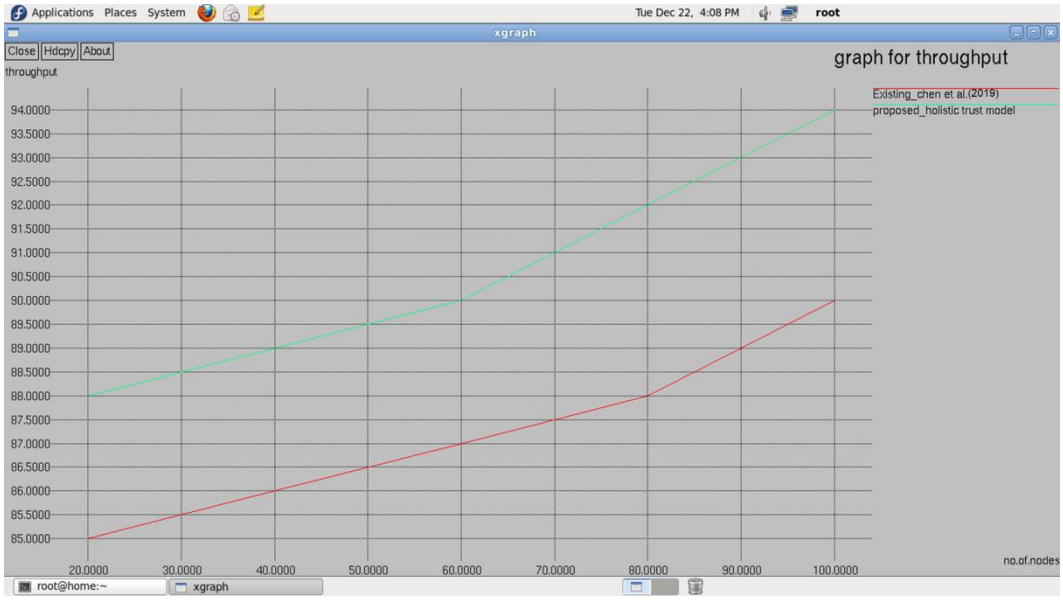

Figure 6. Trust Level (trust level vs. time (sec))

Energy consumption: Figure 7 estimate energy consumption starting energy level to ending energy level. Total residual energy is consumed based on the number of network selection nodes. Here the selections of active sensor nodes are determining the average energy consumption rate. The proposed process makes the lesser energy consumption. In proposed model energy consumption is minimized compared to existing method.

$$Energy\ Consumption = Initial\ Energy - Final\ Energy$$

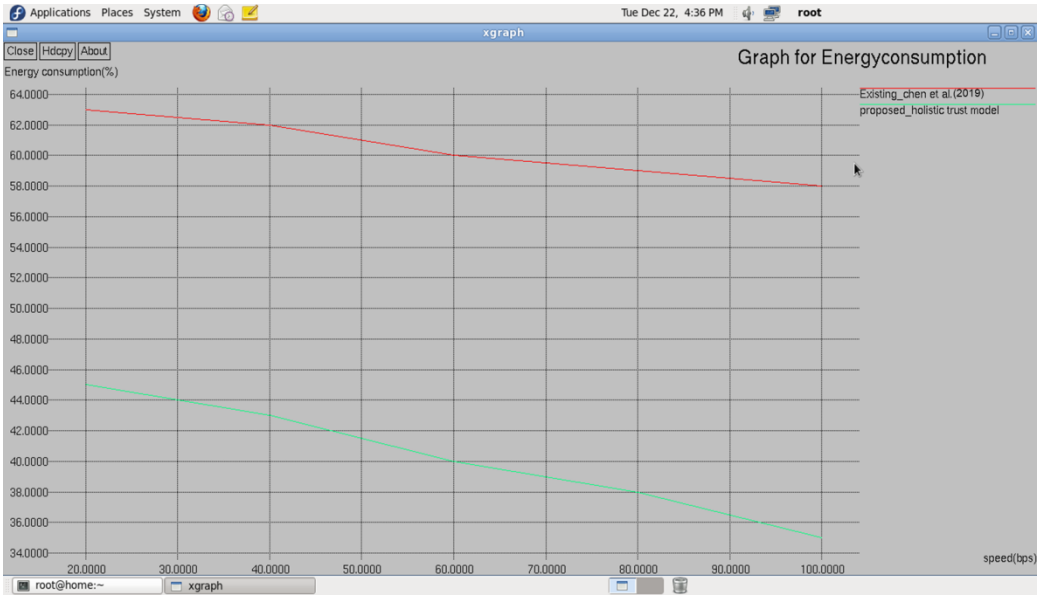

Figure 7. Energy Consumption (energy consumption (%) vs. speed)

Conclusion

Our approach embodies the cluster chaining to form trustworthy zones and then, node migration applied to IoT heterogeneous network achieved the anticipated success resolving trust related attacks, to maintain balanced network and provided new direction to edge computing research world, further different network parameters are considered to select cluster head, than other primitive models where it considers one or two parameters which may not be suitable to judge the head among the nodes. In such situation always high chances are there for selected head node might be wrong one who dissipates the energy quickly, then impacts whole network functionality adversely. Multiple cluster heads architecture is followed inside our cluster to balance the cluster workload and not to overburden the single CH, as implemented in other models. Mainly main cluster head will respond to the instructions given from gateway and updates the status later to it. The other cluster head will facilitate the transfer the sensors collected data to the upstream IoT levels. The whole mechanism is classified as gateway mapped to CH and sensors/transducers mapped to CLCH, finally CH and CLCH will interact with each other to share the tasks and maintain the cluster balanced in terms of residual energy, turn-around time, and memory usage. This approach has unique features to create trustworthy zones, multiple cluster heads architecture and node migration makes its special as compared to other trust level mechanisms analyzed in the state of art.

Conflict of Interest

The authors declared that no conflict of interest.

References

Abhijit J, P., & G. Syam Prasad, D. (2018). Trust Based Security Model for IoT and Fog based Applications. *International Journal of Engineering & Technology, 7*(2.7), 691-695.

Alshehri, M. D., Hussain, F. K., & Hussain, O. K. (2018). Clustering-driven intelligent trust management methodology for the internet of things (CITM-IoT). *Mobile networks and applications*, 23(3), 419-431.

Behera, T. M., Mohapatra, S. K., Samal, U. C., Khan, M. S., Daneshmand, M., &Gandomi, A. H. (2019). Residual energy-based cluster-head selection in WSNs for IoT application. *IEEE Internet of Things Journal*, 6(3), 5132-5139.

Chen, J., Tian, Z., Cui, X., Yin, L., & Wang, X. (2019). Trust architecture and reputation evaluation for internet of things. *Journal of Ambient Intelligence and Humanized Computing*, 10(8), 3099-3107.

Dedeoglu, V., Jurdak, R., Putra, G. D., Dorri, A., & Kanhere, S. S. (2019, November). A trust architecture for block chain in IoT. In Proceedings of the 16th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services (pp. 190-199).

Fernandez-Gago, C., Moyano, F., & Lopez, J. (2017). Modeling trust dynamics in the Internet of Things. *Information Sciences*, 396, 72-82.

Juneja, A., Juneja, S., Bali, V., & Mahajan, S. Multi-Criterion Decision Making for Wireless Communication Technologies Adoption in IoT. *International Journal of System Dynamics Applications (IJSDA)*, 10(1), 1-15.

Juneja, S., Singh, S., & Bali, V. (2017). Research Paper on Detection of Attacks in Static Wireless Sensor Networks. *International Journal of Advanced Research in Computer Science, 8*(7), 225-231.

Khanna, T., Nand, P., & Bali, V. (2020). Permissioned Blockchain Model for End-to-End Trackability in Supply Chain Management. *International Journal of e-Collaboration (IJeC)*, 16(1), 45-58.

Krishna, M. B. (2016). Security and trust management for the Internet of Things: an RFID and sensor network perspective. *Cyber-Assurance for the Internet of Things*, 137-162.

Maddar, H., Kammoun, W., & Youssef, H. (2018). Effective distributed trust management model for Internet of Things. *Procedia Computer Science*, 126, 321-334.

Meng, W., Li, W., Su, C., Zhou, J., & Lu, R. (2017). Enhancing trust management for wireless intrusion detection via traffic sampling in the era of big data. *IEEE Access*, 6, 7234-7243.

Mohan, A., & Bhanu Bhaskara, D. (2018). Multi-dimensional trust aware routing for clustered IOT framework. *International Journal of Engineering & Technology*, *7*(4.20), 15-21.

Oumaima Ben Abderrahim, Mouhamed Houcine Elhdhili & Leila Saidane, (2016). Trust based Clustering Architecture for the Internet of Things, *International Journal of Engineering Research & Technology*, 4 (4), 1-5.

Pourghebleh, B., & Hayyolalam, V. (2019). A comprehensive and systematic review of the load balancing mechanisms in the Internet of Things. *Cluster Computing*, 1-21.

Shah, B., Iqbal, F., Abbas, A., & Kim, K. I. (2015). Fuzzy logic-based guaranteed lifetime protocol for real-time wireless sensor networks. *Sensors*, 15(8), 20373-20391.

Tragos, E. Z., Bernabe, J. B., Staudemeyer, R. C., Luis, J., Ramos, H., Fragkiadakis, A., Skarmeta, A., Nati, M., & Gluhak, A. (2016). Trusted IoT in the complex landscape of governance, security, privacy, availability and safety. Digitizing the Industry-Internet of Things Connecting the Physical, Digital and Virtual Worlds. River Publishers Series in Communications, 210-239.

Wang, J. P., Bin, S., Yu, Y., & Niu, X. X. (2013). Distributed trust management mechanism for the internet of things. *In Applied Mechanics and Materials* (Vol. 347, pp. 2463-2467). Trans Tech Publications Ltd.

Bibliographic information of this paper for citing:

Patnaik, Anup, Mallik, Banitamani, & Krishna, M.Vamsi (2021). Cluster Node Migration Oriented Holistic Trust Management Protocol for Ubiquitous and Pervasive IoT Network. *Journal of Information Technology Management*, 13(1), 100-118.