Policy Based Secure and Trustworthy Sensing for IOT in Smart Cities

Dr.J.V.Anchitaalagammai, E.Deepika, U.Dilbar Aara, S.Nivetha Sree, R.Priyadharshini
Assistant professor, IV Year, IV Year, IV Year, IV Year
Dept of CSE, VCET, Madurai

Abstract

The internet of things (IoT), which is recognized as One of the key enabling technology of smart cities generally refers to the network of smart objects, which are embedded with sensing, computing, networking, and actuating capabilities that all together enable them to collect and exchange data. The IoT devices are usually wirelessly networked and they serve as a key enabling tool for many critical smart city applications such as intelligent transportation, smart grid, smart building, and mobile healthcare. However, security has become a key challenge for the wide deployment of IoT: because of the environmental influences, the IoT data are intrinsically noisy. Moreover, the IoT devices may be compromise by attackers to intentionally generate fake data. Finally, the underlying wireless network can also be subvert. To address the security concern in IoT, we propose a policy-based secure and trustworthy sensing scheme for IoT named Real Alert, in which the trustworthiness of both data and the IoT devices are evaluate based on both the reporting history and the context in which the data are collected using policy rules. Experimental results have shown that the Real Alert scheme can exactly assess the trust of the sensor nodes as well as data in IoT**.**

I.INTRODUCTION

Due to the fact that world urbanization continues to grow
with the estimated total population doubling by 2050, there is a worldwide trend toward Smart Cities. Technological advances in consumer electronics and wireless communication technologies have lead smart devices to serve ubiquitous computing and distributed sensing in smart city applications.
One of the key enabling technologies for smart city applications is Internet of Things (IoT), which generally refers
to interconnect smart objects by extending the Internet technologies. IoT is widely deploy in various smart city application scenarios, such as smart grid, intelligent transportation, and smart building. In IoT, data are collected from various physical sensors, transmit over wireless networks, and then analyzed in a (near) real-time manner. The sensed and analyzed data will be utilized to control actuators. Therefore, security is a critical factor that must be guaranteed in IoT, and we should also ensure high trustworthiness for IoT data. However, the following unique features of IoT have made it difficult to ensure the security and trust for IoT.

- Vulnerable and error-prone transmission medium.
- Untrustworthiness in IoT sensor data.
- Ever-changing network topology.

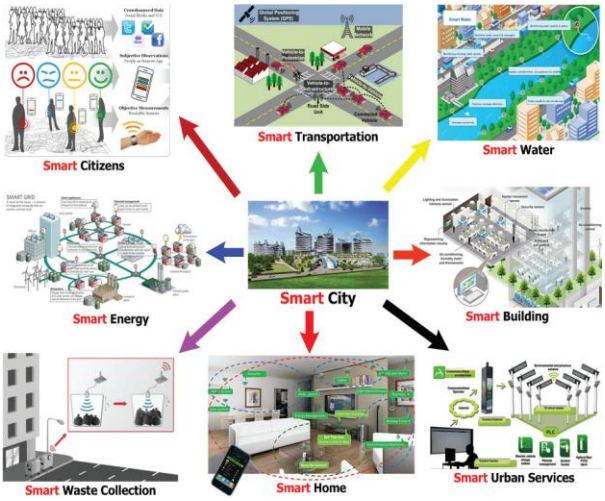


Fig. 1. Various Smart City Applications

II.LITERATURESURVEY

In recent years, various research works have been made to address the security and trust issues in IoT.Survey focuses on identifying how various algorithms have been implemented and its performance. Many related works are as followed.

A. Policy-based Secure and Trustworthy Sensing for Internet of Things in Smart Cities .

This paper was published by Wenjia Li, Houbing Song, and Feng Zeng in 2016.He published this at the International Journal of Computer Applications, He used Dempster's Shafer's theory. He observed that the experimental results have shown that the Real Alert scheme can accurately access the trust of

the sensor node and data in IOT. This was used to detect the malicious nodes and trustworthiness of the data.

B.Secure Data Transmission using AES in IOT

This paper was published by Poonam Dabas and Deepika Khambra.They published this in the International Journal of Application in Engineering on June 2017.The algorithm used by him was the Advanced Encryption Standard(AES).They observed that it enhanced the private key to generate more secure encrypted key through which the devices can transmit data in a secure manner. But the main disadvantage was that it does not reduce the end-to-end delay during secure data transmission.

C.Trust management method to detect On-Off attacks in the IOT

This paper was published by Jean Caminha,Angelo Perkusich and Mirko Perkusich.They published this in International journals on security and communication networks,2017.The algorithm used was machine learning. They observed that this method was able to identify On-Off attackers and fault nodes with a precision up to 96% and low time consumption. The main disadvantage was that it was not intended to identify Ballot stuffing attacks and Bad mouth attack.

III.PROBLEM DESCRIPTION

Security is the big problem because third party can have possibility to access our information or output data. Smart city project is not popular in urban area. So data loss is possible while transferring some data. There is no cryptographic technique while file transformation, so there is no security in data transfer. There is no reliability and efficiency while predicting result. To overcome the problem, we are going to derive some new algorithm in the name of enhanced DST.

IV.EXISTING SYSTEM

In existing system, a trust management scheme for IOT which is based on service oriented architecture (SOA), and the trust management scheme uses the adaptive filtering technique to integrate direct trust and indirect trust to reduce both convergence time and trust estimation bias in the existence of malicious nodes. In the existing algorithm, time delay is too large and so we will be able to identify it only after the attack of malicious nodes, but we cannot detect it.

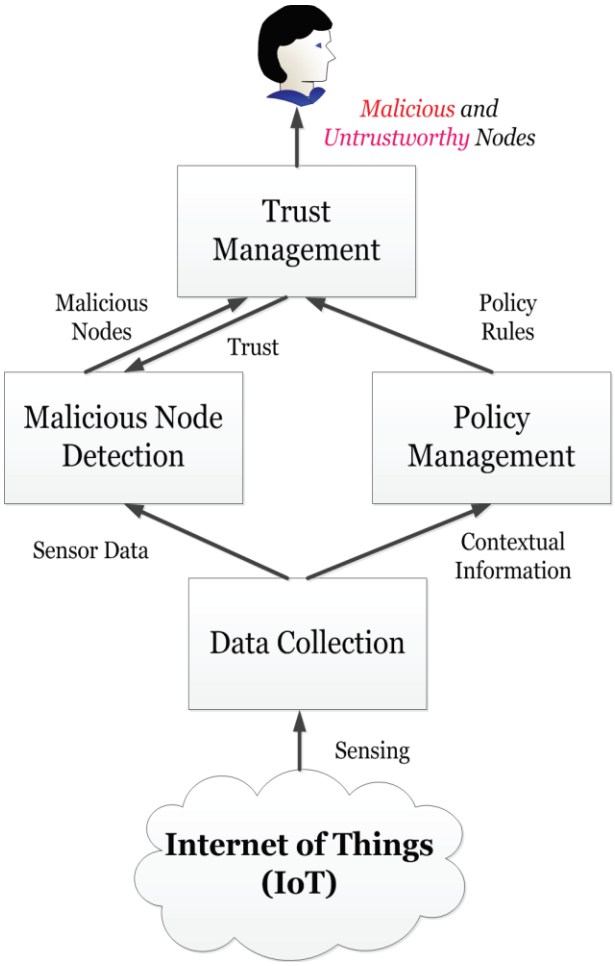
V. POLICY-BASED SECURE AND TRUSTWORTHY SENSING

In this section, we describe the Real Alert scheme in details.

The goal of this scheme is to accurately evaluate the trustworthiness of the IoT nodes and detect malicious ones in different contexts using policies.

A. Scheme Overview

In the proposed scheme, there are mainly four components,
Which are Data Collection, Malicious Node Detection, Trust
Management and Policy Management. The below figure illustrates the proposed scheme.



B. Adversary Model

In this paper, the adversary is supposed to be able to
Compromise IoT sensors, and the compromised sensors can
be used to generate and report fake data, so that the overall
IoT data collection, analysis and decision making process may
be disrupted.
More specifically, we assume that an adversary in general

can perform attacks against the communication protocol to
disrupt the general network operations. However, it is generally the case that such attacks are handled by the intrusion detection techniques, and will thus not be addressed in this paper.
In this paper, we are primarily concerned with trust-related attacks that can disrupt the trust management system. In Particular, we have taken a traffic application where the data collection is very sensitive, so we need to provide security.ie) to identify each node is trustable or not trustable.
• Bad-mouth attack (BMA): a malicious node can ruin the trust of a well-behaved device by providing bad recommendations against it so that the attackers can remain undetected.
• Ballot-stuffing attack (BSA): a malicious node can boost the trust of another malicious node by providing good recommendations for it so that the malicious node can stay in the IoT network for a longer period of time and do a greater harm to the network.
• On-and-off attack (OA): an attacker can occasionally alter their malicious behavior patterns so that it is even harder for the trust management scheme to detect them. For example, they can conduct malicious behaviors for a given period of time and then stop for a while (in that case the malicious behaviors are conducted in an on-and-off manner). In addition, the sly attackers can also exhibit different behaviors to different neighbors, which can lead to inconsistent trust opinions to the same node among different neighboring nodes. Because it is much more challenging to collect enough evidence to accuse the sly attacker (especially when the sly attacker is constantly moving), it is generally more difficult to identify these sly attackers.

C. Data Collection

The Data Collection component collects and then sends the
IoT data to either Policy Management or Malicious Node Detection.
Contextual information is sent to Policy Management, such as velocity, temperature, weather condition, geographic location, etc. In contrast, IoT sensor data are sent to Malicious Node Detection so that the malicious IoT nodes are detected by analyzing these data in traffic application.

D. Policy Management

We apply the collected contextual information to declare
policies in the policy management. For instance, if an IoT node starts reporting abnormal data, then the relevant contextual information will be used to determine whether or not contextual factors are the reason for these abnormal readings. More specifically, we apply the collected contextual information to security policies so as to differ malicious IoT nodes from those misbehaving yet faulty ones. In the Real Alert scheme, the policy rules that can well represent the known ground truth in IoT systems are defined by human experts. For instance, it is obvious that an IoT node is more likely to malfunction if it is moving at a high velocity. Thus, we can define a policy rule like "If an IoT node is traveling at a high velocity then lower the trust punishment for reporting abnormal readings."
Based on these policy rules, the Policy Management component can properly decide if the anomalous IoT data are
resulted from contextual factors, or they may be deliberately
disseminated by adversaries. As a result, this decision will
be used by the Trust Management component to evaluate the
trustworthiness of the IoT nodes.

E. Malicious Node Detection

In the proposed scheme, the statistical outlier detection approach is applied to detect the malicious nodes for IoT in a distributed manner. Outliers generally refer to the data samples that diverge drastically from the remaining data samples. The distributed outlier detection approach is implemented using the following three steps, which are local data collection, data exchange, and data aggregation. The first step of the approach is the local data collection, in which IoT nodes observe and collect the anomalous network activities of other IoT nodes within their transmission range. Each IoT node then summarizes its local data report regarding the top k outliers in its neighborhood. The second step of the algorithm is to exchange the local data of outliers. Each IoT node will broadcast its local data of outliers to its direct neighbors (i.e., IoT nodes that are within its direct communication range).The third step is data aggregation. In this scheme, we use theDempster-Shafer Theory of evidence (DST) to aggregate
the local data and external data received from other IoT nodes.

F. Data Fusion

Dempster-Shafer Theory (DST) is proven to be capable of effectively fusing together multiple data even if some of them is not accurate. In DST, an uncertainty interval that is bounded by both belief (bel) and plausibility (pls) is defined instead of the traditional probability concept. More specifically, bel is defined as the lower bound of this interval and it stands for the supporting evidence. In contrast, pls is the upper bound of the interval and it stands for the non-refuting evidence. For example, if a node Nk observes that one of its neighbours, say node Nj, has dropped packets with

probability p, then node Nk has p degree of belief in the packet dropping behaviour of node Nj and 0 degree of belief in its absence. Moreover, the belief value with respect to a specific event αi and observed by node Nk is calculated as follows.

$$bel_{N_k}(\alpha_i) = \sum_{e:\alpha_e \in \alpha_i} m_{N_k}(\alpha_e)$$

Here αe represents all the basic events that compose the event αi, and mNk (αe) stands for the view of the event αe by node Nk. In this case, since node Nk only get one single report of node Nj from itself, i.e., αi ⊂αi. Therefore, we can derive that belNk (αi) = mNk (αi). Note that ¯ αi denotes the non-occurrence of the event αi. Since the equation
pls (αi) = 1 −bel(α'i) holds for belief and plausibility, we can further derive the following: belNk(Nj) = mNk (Nj) = p and plsNk(Nj) =
1 − belNk (N¯j) = 1.
Therefore, we can combine reports from different nodes by using the Dempster's rule, which is defined as following.

$$m_1(N_j) \bigoplus m_2(N_j) = \frac{\sum_{q,r:\alpha_q \cap \alpha_r = N_j} m_1(\alpha_q) m_2(\alpha_r}{1 - \sum_{q,r:\alpha_q \cap \alpha_r = \Phi} m_1(\alpha_q) m_2(\alpha}$$

G. Trust Management

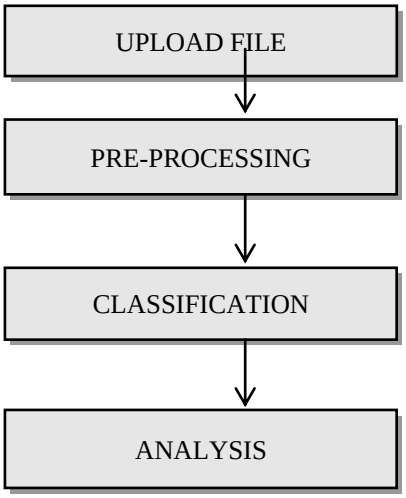
In the Real Alert scheme, we evaluate and manage the trust Of each IoT node in a distributed manner. In addition to the Trustworthiness of each IoT node, we also want to check to see whether or not the collected sensor data are authentic. In intelligent transportation system, we need to know whether or not there is any accident on that road. If so, it is necessary that more actions should be taken, such as sending out an ambulance, issuing traffic alerts, and redirecting incoming traffic,etc.

To address the need of keeping track of the trustworthiness of both IoT nodes and the collected data in IoT, we introduce a new type of trust for IoT in this scheme, namely Data Trust, to indicate the trustworthiness of the IoT data, which is believed to be a valuable addition to the traditional Sensor Trust. For the assessment of Data Trust, we first check if there is any abnormal sensor data (i.e., outlier), which deviates significantly from other sensor data in the vicinity (For example all the velocity data from the sensors of your neighbouring cars). If not, then the sensor reading is trustworthy because it is consistent with readings from nearby devices. However, if there is any abnormal sensor reading, then the next step is to identify if there is any environmental factor that causes the abnormal reading, and we also need to check the trustworthiness of the sensor which sent this abnormal reading.

VI.PROPOSED SYSTEM

We overcome the problem in the existing system by deriving a new algorithm in the name of the enhanced DST.
By using enhanced DST algorithm, any malicious node will automatically get detected and a notification will be triggered. Hence accuracy will be improved.
We get the exact solution using an enhanced DST technique which aggregates the local data and external data received from other IOT nodes. In this system, a series of modules are followed such as,

- Upload file
- Pre-processing
- Classification
- Analysis



MODULES

Upload file:

Upload the smart city dataset containing the city Traffic information connected to SQL.This is the input data; we can cluster the dataset file. The data set contains information from sensors using the smart city and information. We can view the uploaded dataset in a table format.

Pre-processing:

After uploading the file, the unnecessary spaces need to be removed. Preprocessor is used for avoiding the empty space. Data pre-processing consists of a series of steps to transform the raw data derived from data extraction. These databases can have many quality

control issues.Pre-processing aims at assessing and improving the quality of data to allow for reliable statistical analysis.

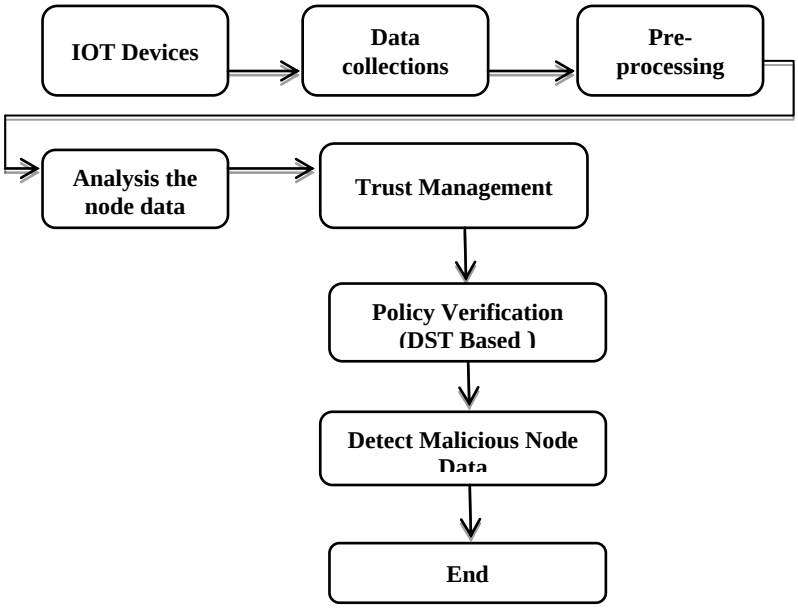
Classification:

DST Algorithm

DST is used to aggregate the local data and external data received from other IOT nodes. The DST based data aggregation method is proven to be capable of effectively fusing together multiple data even if some of them is not accurate. In DST, an uncertainty interval that is bounded by both belief (bel) and plausibility (pls) is defined instead of the traditional probability concept.

Analysis:

The data from the nodes will be analysed and then those data will be combined for confidentiality, i.e. (belief (bel) and plausibility(pls)).From the analysis, if belief node is higher than the plausibility node, then there are no malicious nodes.But if plausibility is higher, then the nodes are malicious.



VI.REQUIREMENTS

Hardware requirements:

System : Pentium dual core
Hard Disk : 160 GB
Monitor : 15 VGA color
Mouse : HP
Keyboard : 110 keys enhanced

Software requirements:

O/S : Windows 7/8
Language : Java
Tool : Wamp server
IDE : Net-Beans 8.0
Database : MySQL

VII. PERFORMANCE EVALUATION

To validate the effectiveness of the proposed scheme, Glo- MoSim 2.03 is adopted as the experimental platform, and the simulation parameters. In the experiments, each IoT node will initially sense and record contextual information, including travelling speed, temperature, altitude, and so on, so that it is fully aware of the surrounding context in order to evaluate the trustworthiness of the neighbouring IoT nodes more accurately. To compare the performance of the proposed scheme with some well known existing solutions, we pick the lightweight trust management method without using any security policy as the baseline approach. In the experiments, the following two parameters are used to indicate the accuracy of the Real Alert scheme: Precision (P) and Recall (R), as defined below:

$$P = \frac{Num\ of\ Truly\ Malicious\ Devices\ Caught}{Total\ Num\ of\ Untrustworthy\ Devices\ Caught}$$

$$R = \frac{Num\ of\ Truly\ Malicious\ Devices\ Caught}{Total\ Num\ of\ Truly\ Malicious\ Devices}$$

Each simulation scenario is executed for 30 times with different random seeds, which guarantees a unique initial node
placement for each time. Then, the experimental result is the
average over the 30 runs for each simulation scenario.

A. Effect of Various Parameters on Real Alert

The first set of experiments aim at evaluating the effect of different parameters, such as node density, percentage of Malicious nodes, and node mobility, on the RealAlert scheme. The RealAlert scheme achieves a higher precision value than the baseline method when node density varies. Moreover, when the device density is higher, both methods yield a better precision. The rationale behind this result is that it is more possible to receive authentic data from IoT nodes when there are more IoT nodes.

The RealAlert scheme outperforms the baseline method for the recall value. Also, the recall value is higher when the device density is higher. It takes less time for RealAlert to find the malicious IoT nodes than the baseline method when the number of nodes in IoT varies. This is true because we apply policy rules in our scheme to integrate the contextual factors when we

distinguish malicious IoT nodes from faulty/malfunctioning ones.

The precision and recall values both degrade when there are more malicious nodes in the IoT network, which is easy to understand. Moreover, the RealAlert scheme is able to yield a better performance than the baseline method for both precision and recall values in the presence of more malicious IoT nodes. Moreover, the RealAlert scheme achieves a better time efficiency than the baseline method regardless of how many
Malicious IoT nodes there may be.

The performance of the RealAlert scheme when the IoT nodes travel at different speeds, and we observe that the RealAlert scheme outperforms the baseline algorithm, and even at a high travelling speed (20 m/s), it can achieve pretty good precision and recall values.

B. Effect of Attack Patterns on RealAlert

In addition to investigating the effect of different parameters, we are also interested in knowing the impact of different attack patterns, such as BMA, BSA, and OA.It is obvious that the RealAlert scheme achieves a better performance than the lightweight trust management scheme regardless of which attack pattern is utilized.

It shows that the performance of the lightweight trust management approach degrades significantly under the BMA pattern especially when there are a large amount of malicious nodes in the IoT network, whereas the RealAlert scheme still achieves over 80% of precision and recall scores even when there are 40% of malicious nodes which are conducting bad mouth attacks.

It is worth noting that the bad mouth attack aims to intentionally make wrong trust recommendations so that the malicious nodes can remain undetected for a longer period of time and the benign nodes will be falsely accused of malicious behaviours. Therefore, it is of great importance that the proposed RealAlert scheme is resilient to the dangerous bad mouth attack. Moreover, when a sly attacker launches the on-off attack, in which the malicious behaviours are conducted in a more intermittent manner.

To make things worse, the attacker can exhibit different behavioural patterns to different nodes. Thus, it is inherently more difficult to detect the untrustworthy behaviours in this attack pattern. We find from that the RealAlert scheme can still perform well in terms of high precision and recall scores in presence of 40% malicious nodes. On the other hand, the precision and recall scores yielded by the baseline trust management scheme become significantly lower when the percentage of malicious nodes increases.

To summarize, we can clearly conclude that the RealAlert scheme is resistant to different and advanced attack patterns. In addition, it can also tolerate the high percentage of malicious nodes in the IoT network.

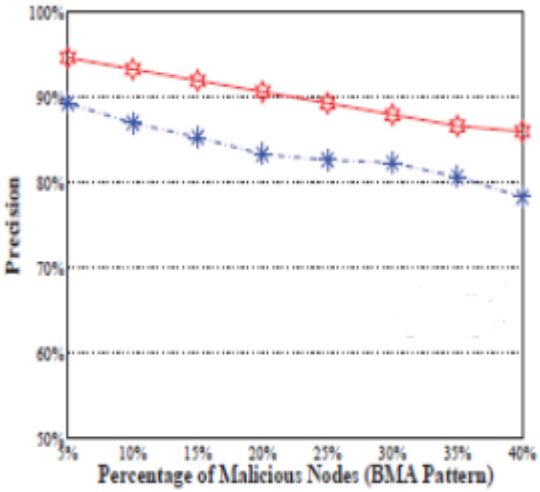
VIII.CONCLUSION

Security and trustworthiness are generally regarded as the two key challenges for the successful deployment of Internet of Things (IoT). To address the urgent need of trustworthy and Secure sensing in IoT, we propose a policy-based secure and Trustworthy sensing scheme named Real Alert.

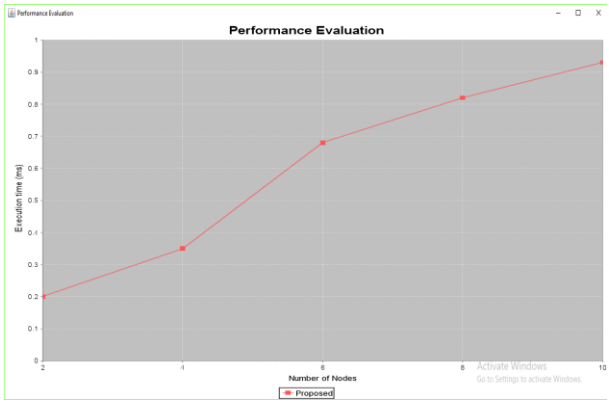
If any of these attacks occurs in traffic environment, then the entire traffic application will be spoiled. So we are going to find the trusted node by providing high level of security. Everything was under cryptographic techniques ie) encrypting the data, so we are moving to trust management that is transfer of data is only to the trusted node.

In the RealAlert scheme, the trustworthiness of both the data as well as the IoT nodes which generate those data are assessed using the anomalous IoT data and also the contextual information that represents the environment under which anomalous IoT data are obtained. In order to represent and leverage the contextual information in a more accurate fashion, some policy rules are defined to specify how we evaluate the trustworthiness in different situations. Experimental results demonstrate that the RealAlert scheme is able to determine the trustworthiness of both IoT nodes and data in an efficient and accurate manner.

COMPARISION OF GRAPHS



PERFORMANCE GRAPH



REFERENCE

[1] G.Cardone, A. Cirri, A. Corradi, and L. Foschini, "The participact mobile crowd sensing living lab: The testbed for smart cities," IEEE Communications Magazine, vol. 52, no. 10, pp. 78–85, October 2014.

[2] F.J.Wu and H. B. Lim, "Urbanmobilitysense: A user-centric participatory sensing system for transportation activity surveys," IEEE Sensors Journal, vol. 14, no. 12, pp. 4165–4174, Dec 2014.

[3] H.Song, R. Srinivasan, T. Sookoor, and S. Jeschke, Smart Cities: Foundations, Principles and Applications. Wiley, 2017.

[4] K.Rogers, R. Klump, H. Khurana, A. Aquino-Lugo, and T. Overbye,"An authenticated control framework for distributed voltage support on the smart grid," IEEE Transactions on Smart Grid, vol. 1, no. 1, pp.40–47, June 2010.