SMART: a Secure Remote Sensing Solution for Smart Cities' Urban Areas

Geetanjali Rathee, Chaker Abdelaziz Kerrache, Carlos T. Calafate, Muhammad Bilal, and Houbing Song

***Abstract*—Nowadays, smart cities are becoming an emerging area of research for upgrading and modifying our existing society by adopting the latest and the most trending technologies in the market. Though the number of IoT based applications is constantly increasing, with new products being launched every 6 months, many organizations are afraid of an early adoption of such products because of their security issues. In particular, the transmission and storage of online information causes a lot of cybersecurity issues while ensuring a secure communication mechanism. The aim of this paper is thus to present an efficient and effective communicating mechanism for smart cities using two decision-making models based on the SMART and Subjective approaches. The SMART approach is used to make an intelligent and ideal decision when communicating in the network. In addition, the continuous surveillance of the communicating entities can be done by computing their trust values through a subjective mechanism. The devices having a higher trust value are thus considered as more trustworthy devices. The proposed mechanism is simulated and verified for various security metrics, being compared to the state-of-art approaches. In addition, the proposed mechanism is simulated and out-performed against existing approaches by showing a 97% improvement in terms of accuracy, utility value, delay and threat metrics.**

***Index Terms*—IoT, SMART, Indirect trust values, security scheme, remote sensing, smart cities.**

I. Introduction

Urban planning is considered as a significant element towards the development and modernization of smart cities [1]. It basically encompasses the planning, layouts and construction of new buildings, along with development directions for implementing a new concept of regional city. It requires involving Internet and computer-based technologies/software in order to understand the whole information of smart cities including a geographical perspective. [2]. The goal and motivation of developing and constructing smart cities is to design and efficient communication environment with minimal human involvement. In the practical construction process of developing urban areas for designing smart cities, it is important to understand every single aspect of the communication process. The construction of smart cities includes tons of information being generated, followed by their storage and automatic decisions by analyzing the data using various recent techniques like Data Mining and Large Language Models. This way, smart cities, where the handling of information is done through various intelligent and smart devices to take an independent decision, is done without any human involvement [3]–[5]. A number of countries have been attracted towards this concept, especially in urban areas where it is very difficult to interact physically or on a regular basis [6], [7]. Hence, remote sensing techniques are used in places that cannot be easily reached by humans. In those cases, smart sensors and drones can be easily deployed and implemented for continuous surveillance, enabling devices to participate in taking immediate decisions [8]–[10].

Many counties adopted this concept of using remote sensing in urban areas as a first step towards smart cities' development. However, the deployment and modification of information cannot be easily done with the threat of cyber criminals and intruders. Figure 1 presents an architecture for smart cities where urban areas are under surveillance, and where activity recognition of any kind relies on remote sensing techniques in order to establish an efficient and effective communication mechanism [11], [12]. The first phase mentions the remote sensing and computation phase that gathers the huge amount of information generated by 'n' number of devices in the network. In addition, during phase two, the security approaches are implemented in order to categorize the devices. Finally, the third phase makes an accuracy prediction, and analysis of records generated by legitimate devices in the network.

A. Objective

When deploying networks acting as Smart City infrastructures, a high number of cyber threats may be encountered, enabling intruders to launch a myriad of possible attacks. The involvement of various communicating devices, including smart devices, smart alarms, etc., enables intruders to compromise the legitimate intelligent devices in the network in such a way that they may start behaving according to the intruder's intention [13]–[15]. For instance, compromised communicating devices miners may sense incorrectly or drop the packets during the broadcasting or forwarding of information in the network. Compromised smart devices may further affect the network performance by breaching confidentiality, access

(Corresponding Author: Chaker Abdelaziz Kerrache)

Geetanjali Rathee is with the Department of Computer Science and Engineering, Netaji Subhas University of Technology, Dwarka Sector-3, New Delhi-110078, India. (e-mail: geetanjali.rathee123@gmail.com)

Chaker Abdelaziz Kerrache is with the Laboratoire d'Informatique et de Mathématiques, Université Amar Telidji de Laghouat, Laghouat, Algeria. (e-mail: ch.kerrache@lagh-univ.dz)

Carlos T. Calafate is with the Computer Engineering Department (DISCA), Universitat Politècnica de València, Valencia, Spain. (e-mail: calafate@disca.upv.es)

Muhammad Bilal is with the School of Computing and Communications, Lancaster University, Lancaster, United Kingdom. (e-mail: m.bilal@ieee.org)

Houbing Song is with the Department of Information Systems, University of Maryland, Baltimore County (UMBC), Baltimore, USA. (e-mail: songh@umbc.edu)

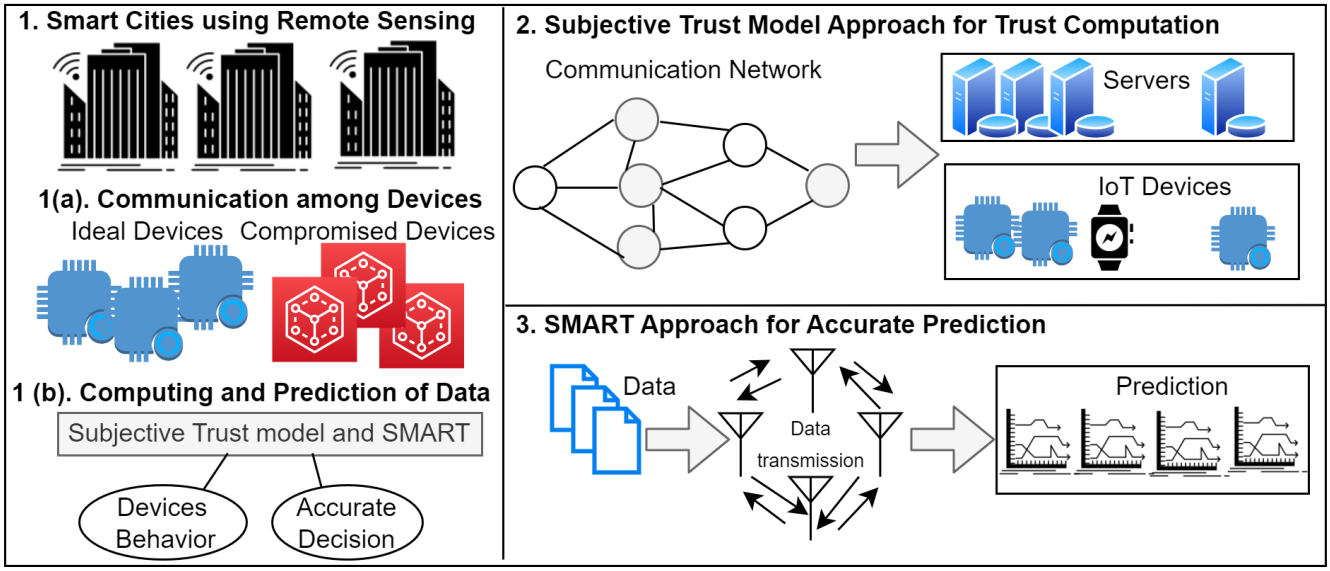

Fig. 1. Remote Sensing framework.

control and integrity. Preventing the disclosure of generated information, along with client validation, are critical issues that should be addressed before starting the communication process in the network. In addition, the availability of the required resources by legitimate devices is further significant for ensuring an efficient and effective network communication mechanism. The existing security mechanisms/techniques and methods tried to achieve an efficient communication mechanism using remote sensing techniques for surveillance of the urban areas for smart city construction.

B. Contribution

The goal of our proposed solution is to provide an efficient and accurate communication mechanism to identify dishonest devices in the network. The proposed framework integrates two different approaches to ensure the confidentiality, integrity and availability of the resources in the network. Initially, we use a subjective mechanism for categorizing the communicating devices into malicious and altered. The subjective approach provides the confidentiality for recognizing the legitimate devices, and to prevent accepting as valid any information coming from malicious devices. Furthermore, the subjective approach is integrated with the SMART technique for ensuring an adequate availability and accuracy of the decision-making process in the network [16], [17]. The real-time decision making procedure seeks to identify legitimate devices during the regular communication process; this is achieved without overwhelming the network with additional overheads. The proposed mechanism performance is analyzed and validated using various security and networking parameters including accuracy, replay attack, utility value and delay. Thus, we briefly explain the contributions of our study in below points:

- The subjective approach is used to ensure the confidentiality when recognizing legitimate devices, while excluding the messages coming from malicious devices.
- The subjective approach is then integrated with the SMART technique to ensure the availability and accuracy of the decision-making process in the network.
- The proposed mechanism is further analyzed and validated against various security metrices in terms of accuracy, cheating threats, utility value and delay.

The remainder of this paper is structured as follows: a literature review discussing a number of security models is presented in section 2. A detailed explanation of the proposed mechanism, along with the proposed methodology, system model, and algorithms, is detailed in section 3. Afterwards, section 4 validates the proposed solution using various security measures, including a comparison against the existing approach. Finally, section 5 concludes the paper and discusses future directions.

II. Related Work

Though a number of security schemes or frameworks have been proposed by various researchers [18], [19]. However, it is very critical to ensure trust integrity and confidentiality in the network with upgraded network performance in terms of accuracy, counter cheating attack (replay attack), utility value, and delay. This section discusses the main existing approaches in the literature having as a main aim to ensure an accurate and reliable communication among devices. The discussed solutions are also highlighted in Table I.

Yaakob et al. [20] designed a cost effective IoT-based remote sensing prototype for monitoring a patient's health, providing a continuous surveillance of the patients, where sensors are integrated with Arduino UNO controllers for the processing of information. The authors tried to overcome the burden of looking over the patients physically by having medical professionals remotely monitoring the patient's health. In another work, Simplicio Jr. et al. [21] proposed a lightweight security framework for providing several services. In particular, while transmitting or storing the information,

the proposed mechanism easily tracks the mobile health information gathering, along with the protection of the data by a multi-agent duplication approach.In addition, the proposed system has been deployed and tested in a real-time scenario located in Sao Paulo, Brazil.

Rahman et al. [22] proposed a multi-tier lightweight secure communication mechanism among end nodes.They presented a secure Message Query Telemetry Transport mechanism based on a cipher text/key attribute encryption mechanism using the ECC cryptosystem. In addition, they introduced a multi-tier communication mechanism along with an extra security layer. Liu et al. [23] investigated various multi-source heterogenous information gathering for the public data platform. Afterwards, they focused on the integration of data and sharing by introducing warehouses and application deployment. The aim of the multi-source information gathering is to continuously update services' multimedia information in real time. Brisimi et al. [24] explored new variants for sensing and classifying roadway obstacles by introducing some appropriate regularization. The authors used classification and clustering algorithms to sense the obstacles. In addition, the authors presented novel metrics based on actual/real data computation. Finally, they used Boston's city roadmap for verifying and checking the affectability of their system. Chen et al. [25] developed a framework for urban and spatial network for ensuring the sustainability based on smart cities. With the launch and continuous development of high-resolution images, the satellite has covered various chromatograms such as panchromatic, multispectral and hyperspectral. The authors used a state-of-the-art approach to construct an efficient model. They then analysed the remote sensing services, and updated the processed data by designing an urban model for smart cities. The proposed mechanism is verified through experimental tests against different scenarios. Finally, Hendy et al. [2] developed an ICT framework for smart cities to achieve their goals. The authors did a literature review, and have chosen Dubai as a case study by identifying the determinants, subdimensions, etc. The paper also arranged the entire group into seven basic dimensions.

A. Problem Statement

Though a number of schemes and approaches have been proposed by various researchers and engineers, existing mechanisms still face certain computational and storage overhead issues. In particular, existing approaches require complex computations in order to provide security that may further introduce long delays, lack of accuracy, and increased storage overheads in the network. In this regard, the proposed solution provides better security by introducing less delays and providing more accuracy by detecting the legitimacy of devices during the information transmission process.

III. Proposed Model

A. System Model

The modernization of urban areas is considered as the main part and the future of smart city deployment to learn the future directions, layout and city construction. For modelling the generated information from the surroundings, and take an accurate and correct decision at once, there is always a possibility of an intruder's invention with the aim of degrading the network performance. The involvement of malicious devices during the information gathering, analysis of the data, and decision-making processes, not only affects the communication mechanism, but also leads to generating a threat on organizations when adopting new technologies. Therefore, it is fundamental to protect and secure each communicating device/sensor while transmitting the information in the network. The system model of proposed scenario consists of number of IoT devices as $I0, I1 \ldots In$ that communicate and interact with each other in a network size of 'n' devices. The system block diagram of the proposed framework is depicted in Figure 2 having two different approaches to provide an accurate and trustworthy decision-making process. The horizontal dots represent additional analysis and computations task done by the devices during the processing of information in the network. In addition, the vertical dots represent the division of processes done during the information processing. The top phase presents the tasks performed by 'n' number of devices; the middle phase presents the implementation of security approaches over 'n' number of devices. Finally, the bottom phase presents the category of devices (either legitimate or malicious) after assessing their nature.

The diagram shown in Figure 2 consists of 'n' IoT devices that generate, transmit and process a large amount of data from their surroundings. The collected information is further processed and analysed using two different approaches, such as SMART, i.e. Simple Multi-Attribute Rating Technique, and a subjective trust model. The subjective model is considered as the trust model approach for analysing the communication history or behaviour of the device. There is a number of ways to determine the communication history of a model, and where trust is considered as one of them, being considered the most adequate approach without adding any extra cost for the security layer when analysing the behaviour of each communicating device [26]. The trusted devices are again integrated with SMART for providing an accurate and correct decision making by each communicating device in real time. The decision-making process is considered as a computer-based system where a weight product is integrated for each criterion in order to analyse the entire history of the device. The weights in this approach are termed as the trusted values computed through the subjective approach. The detailed explanation of each security measure, such as the SMART and subjective approaches, is discussed below.

In addition, Table II provides a list of abbreviations before their usage in order to properly understand the workflow of the proposed solution.

B. Subjective Method

The subjective trust model is defined as a direct method of trust computation by directly monitoring the node's experience. The number of data packets successfully transmitted or forwarded by a device, and the number of packets received

TABLE I
LITERATURE SURVEY.

Author's Name	Technique	Performance Metrics	Limitation
Hendy et al. [2]	Developed an ICT framework for smart cities to achieve their goals.	The paper also arranged the entire transmission into seven basic dimensions.	Needs to improve security for real-time transmissions.
Yakoob et al. [20]	Designed a cost effective IoT based remote sensing prototype for monitoring the patient's health.	The continuous surveillance of the patients where sensors are integrated with Arduino UNO controllers for processing the information.	The authors tried to overcome the burden of looking over the patients physically by remotely monitoring the patient's health through medical professionals.
Simplicio Jr. et al. [21]	Proposed a lightweight security framework for providing several services related to security.	The proposed mechanism easily tracks the mobile health gathering of information while promoting or protecting the data from information loss through various agents.	Significant computational delay is introduced.
Rahman et al. [22]	Multi-tier low-weight secure communication mechanism among end nodes.	The authors have proposed a detailed security framework and analysis of information with an enhanced security model that includes improved features.	The system requires complex computation.
Liu et al. [23]	Various multi-source heterogenous information gathering for the public data platform.	The authors have focused on the integration of data and sharing by introducing warehouses and application deployment.	Leads to networking security threats.
Brisimi et al. [24]	Explored new variants for sensing and classifying the roadway obstacles by introducing some appropriate regularization.	The authors have used a classification and clustering algorithm to sense the obstacles.	Authors did not propose any model.
Chen et al. [25]	Security framework for urban and spatial networks for ensuring the sustainability based on smart cities.	The authors have used a state-of-the-art approach to construct an efficient model.	Two-level trust scheme leads to increased security costs.

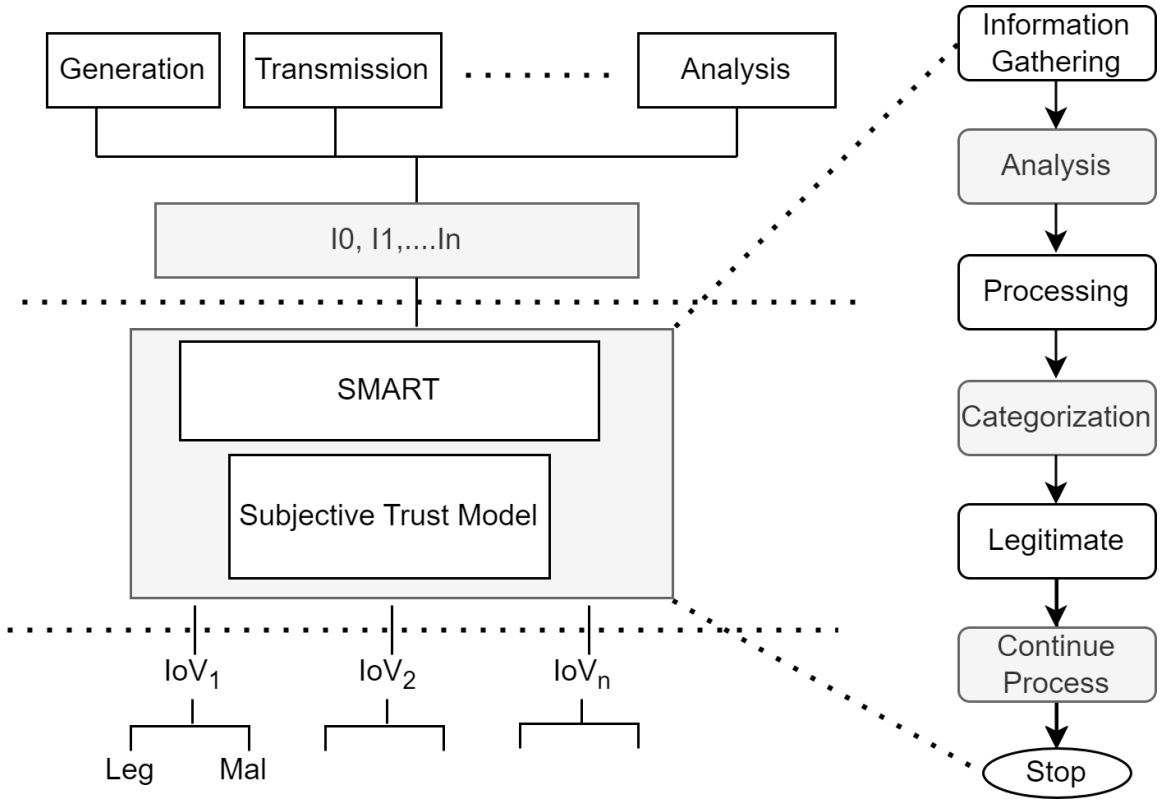

Fig. 2. System Block Diagram.

by that device within time 't', determines the historical observation of each device. In addition, the delay can be raised in the network to analyze relevant communication issues such as congestion, system failures, etc.; in that case, it is necessary to consider a threshold value when determining the trust of each device. To this end, a delayed time decay function for each device can be introduced, where the amount of delay is allowed in the network is defined as:

TABLE II
LIST OF ABBREVIATIONS.

Definition	Value
Decay function	d_f
Device monitoring	m_i
Subjective observation of device i and j	SO_{ij}
Computed decay function	C_f
Computed decay function over time 't'	C_t
Error influence	$V1_{(f)}$
Various differential equation coefficients	a, b, c
Response function	$V^u(f)$
Grey fitting precision index	$y(f)$

$$d_f = \delta^{n-f}, 0 < \delta < 1, 1 < f \leq n \tag{1}$$

Where delta denotes the authentication mechanism which measures the smaller base coefficient. The smaller the value of coefficient, the greater is the attenuation of each value. In addition, at the p^{th} time (t_p), the monitoring device m_i makes a subjective observation according to the equation below:

$$SO_{ij}(t) = \frac{\sum_{f=1}^{m} d_f SOij(t_f)}{\sum_{f=1}^{d_f}} \tag{2}$$

The subjective observation of each device is computed as follows:

$$SO_{ij}(t) = \frac{C_f(t_f)}{C_t(t_f)} \tag{3}$$

Now, after a nonce of time 't', the trust value of each device can be obtained as $TV = TV_{(t1)}, TV_{(t2)} \ldots\ldots TV_{(tn)}$, that can be transformed to a sequence of data generated by devices as $V(0) = v0_1, v0_2, \ldots v0_n$. An average series is generated in order to check the influence of errors during information communication as below:

$$V_1(f) = \sum_{m=1}^{f} V^{-(0)}(m)$$
$$where, x^{-(0)}(f) = \frac{(x^0(m) + x^{(0)}(m-1))}{2}$$

The above equation can be further transformed to:

$$df(m) = ae^{b(f-1)} - c \tag{4}$$

$$b = \frac{ln \sum_{f=1}^{n} V^{-(0)(f-1)V^{-(0)}}(f)}{\sum_{f=3}^{n}(V^{-(0)}(f-1))^2} \tag{5}$$

$$C = \frac{1}{(n-1)}[(\sum_{f=2}^{n} e^{b(f-1)}a - \sum_{m=2}^{n} V^{(1)}(f))] \tag{6}$$

The assumption is determined as $v(1) = a - c$, $U = bc$, and the transformed differential equation can be established as a response function after the reduction process is determined as:

$$V^{(u)}(f) = e^{b(f-1)} 2 \frac{a(1 - e^{-b})}{1 + e^{-b}} \tag{7}$$

As per the above stated equation, in case $f = 1, 2, \ldots n$, the set $v(0)(f)$ presents an fitting sequence in case $f > n$, which means it is a prediction sequence. The grey fitting precision index is further computed as:

$$y(f) = \frac{V^{(0)}(f)}{V^{(0)}(f)} \tag{8}$$

This represents the fit level based on the derivation degree from original sequence.

C. SMART

SMART is a multi-attribute rating mechanism that provides an accurate decision making after considering the trust value from the subjective observation function. SMART is a weighted decision model on a scale from 0 to 1 for computing and comparing the values of each device. The model applied for each device is defined as:

$$M(x_i) = \sum_{a=1}^{n} W_a m_i(x_i), i = 1, 2, ...n \tag{9}$$

The number of steps that the SMART system applies following the subjective observation scheme, according to the function above, are the following:

- Step 1: The number of criteria considered for decision making need to be defined.
- Step 2: The criteria weight is defined as the trust values of each communicating device, and computed through the subjective approach using a 1-100 interval on each criterion.
- Step 3: The normalization of each communicating device is illustrated as the comparison among the device's weight and the actual weights of each criterion as:

$$N = \frac{W_a}{\sum W_a} \tag{10}$$

  Where, W_a is the weighted criteria, and σW_a is the total weight of all criteria.
- Step 4: After providing the criteria parameters for each device, the utility value is converted into a data criterion raw value as:

$$M_i(x_i) = \frac{C_0 - C_i}{C_{max} - C_{min}} \tag{11}$$

  Where, $M_i(x_i)$ is the utility value of a criterion from -1 to I, and C_{max} and C_{min} are the maximum and minimum criterion values. In addition, $C_0(i)$ is the value of minimum criteria.
- Step 5: After determining the $b = values$ for each criterion, the shifting values obtained using normalization, along with their weighted criteria values, are obtained.

The working of the entire proposed mechanism can be easily understood using an Algorithms 1 and 2 as explained below.

IV. PERFORMANCE ANALYSIS

A. Model design

In order to understand the process of information transmission in urban areas through remote sensing mechanisms, we needed to build a well-planned management and construction

Algorithm 1 Secure Remote Sensing Algorithm using Subjective and SMART.

Prerequisite: All the devices are authentic and able to communicate among each other
Input Value: (1) A network N having $N = d_1, d_2, d_3 \ldots\ldots d_n$ number of smart devices
Output: Device is ideal or altered
Given: An effective communication system using subjective and SMART approaches

Step 1: Establish the networking environment.
all nodes $D_d = D = 1, 2, \ldots D$ x=1 to N Compute confidentiality of each communicating device using
Subjective () Model
(Device is ideal)
Maintain a trust level network of legitimate devices and determine their legitimacy and confidentiality
Block/deny further communication
Step 2: Each ideal device is surveilled using SMART

Algorithm 2 Subjective() and SMART() Approaches.

Step 1: The delay of each communicating device is computed using:

$$d_f = \delta^{n-f}, 0 < \delta < 1, 1 < f \leq n \tag{12}$$

Step 2: The subjective observation that is used to analyze the authentication of communicating devices is defined as:

$$SO_{ij}(t) = \frac{\sum_{f=1}^{m} d_f SOij(t_f)}{\sum_{f=1}^{d_f}} \tag{13}$$

The subjective observation of each device is computed as follows:

$$SO_{ij}(t)(t_f) = \frac{C_f(t_f)}{C_t(t_f)} \tag{14}$$

Step 3: Finally, the precision index to measure the confidentiality is computed as:

$$C = \frac{1}{(n-1)}[(\sum_{f=2}^{n} e^{b(f-1)}a - \sum_{m=2}^{n} V^{(1)}(f)] \tag{15}$$

$$y(f) = \frac{V^{(0)}(f)}{V^{(0)}(f)} \tag{16}$$

of the problems and surroundings of a smart city. The complete model design and simulation framework of our proposed mechanism is presented in Figures 3 and 4. Figure 3 presents the designed framework, which must be considered to provide a secure and efficient communication mechanism among devices in the network. IoT devices that gather and generate the information from the surroundings will pass their entire information to base stations, where data will be processed and analysed by applying both the security mechanisms proposed: SMART and subjective methods. Furthermore, the processed and categorized information will be reported, and will be tagged as either legitimate or alternate.

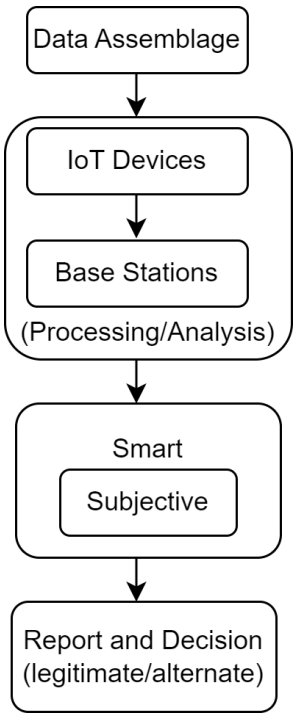

Fig. 3. Proposed framework.

Figure 4 represents the simulation flow where the framework of our proposed mechanism using MATLAB simulation; such framework enables analysing the behaviour of each communication device, and to tag it as either legitimate and malicious. Furthermore, Table IV represents the simulation parameter for verifying and validating the proposed solution.

TABLE III
SIMULATION METRICS FOR VERIFICATION OF PROPOSED APPROACH

Metrics	Value
Total no. of devices	300
Weights	based on TV of device
Devices alteration rate	20%
Varying trusted values of devices	$[0, 1]$
Power of transmission	$[15, 20]$ dBm
Devices types	Legitimate=300, Altered= 60

Now, in order to analyze the behaviour of the network over the time, a measuring parameter known as satisfaction ratio is considered that recognises the stability in the network. Figure 4 presents the satisfaction ratio of the interaction as a function of simulation time. The x-axis represents the count of simulation steps, while the y axis represents the satisfaction of trusted devices. Initially, all the trust models are increasing, and then remain stable in the network after identifying the behaviour of each communicating device.

B. Model Performance

In order to verify the accuracy and validity of our proposed mechanism when compared to existing technologies, a comprehensive test is conducted using MATLAB where 1000 devices, and time of 250 steps, were used to recognize

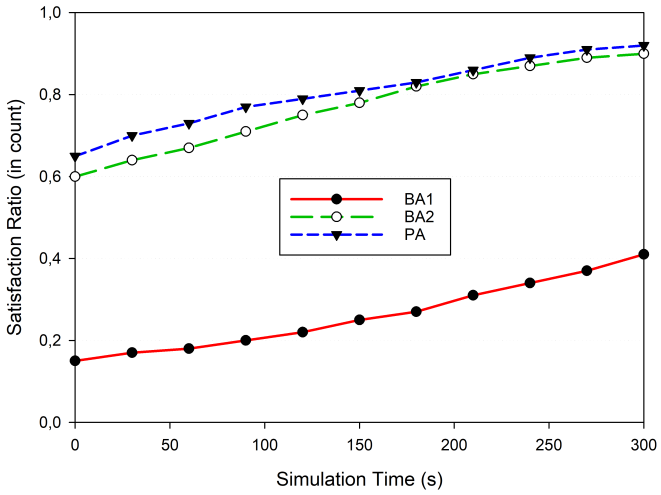

Fig. 4. Satisfaction Ratio.

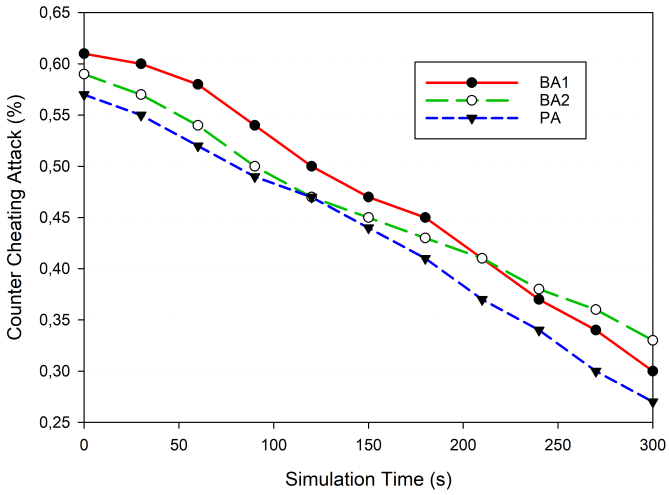

Fig. 5. Cheating Threat.

the behaviour of devices (i.e., legitimate or altered). The validity is proved by dynamically containing the presence of 20% altered devices in the entire simulation while validating the proposed framework. Initially, subjective trust approach is applied to the 1000 devices in order to categorize them as either legitimate and malicious. In addition, the SMART mechanism is applied to further improve the decision-making accuracy when devices are communicating in the network. The immediate response to any device according to the surroundings is handled by SMART mechanism. The devices are aligned with some weights here represented with trust values, and computed through a subjective approach using our criteria. The weighted normalization and parameter values, along with their alternatives, is represented in Table III.

TABLE IV
PROPOSED MODEL PARAMETERS

Criteria	Weight	Parameter Values	Alternatives	Normalization
C1	TV1	Low (1)	A1	TV1/1000
C2	TV2	Mid (2)	A2	TV2/1000
C3	TV3	High (3)	A3	TV3/1000
C4	TV4	Very High (4)	A4	TV4/1000
C5	TV5	Higher (5)	A5	TV5/1000

C. Baseline Methods

The baseline approaches considered for comparing and validating the proposed scheme, BA1 and BA2, are a real-time forest inventory framework [10], and trusted framework for identifying intrusion or data failure [19], respetively. Srividya [19] et al. have proposed a trustworthy resource reservation protocol for identifying the failure in the network. The authors have used a weighted algorithm for reducing the delay by choosing the shortest path. In addition, the simulation results proved the link failure and trust accuracy while transmitting information in the network. Nicholas et al. [10] proposed a fine-scale advanced remote sensing airborne laser scanning for identifying the intruders in the network. The authors have considered real-time data for detecting the error propagation for validating and simulating the results. Our proposed mechanism is simulated against these methods by using the subjective and SMART approaches for sensing the illegal activities in urban areas, thereby ensuring a secure communication system. The trusted approaches of proposed method and existing method is compared and verified in order to identify the validity and out-performance of our work.

D. Results and Discussion

The simulation is done to measure performance metrics that include cheating threats, utility value, accuracy and delay. Figure 5 represents the cheating threat by malicious devices during the communication process. Initially, the altered devices behaves as highly reputed devices with good performance for a specific interval of time, and then started behaving malicious. Figure 5 shows that, as simulation steps increase, our proposed model performs better than existing approaches, as we are continuously monitoring the behaviour of all devices, along with their trust values. The subjective approach identifies the behaviour of each node as early as possible by detecting their internal features such as activeness, behaviour, resource requirements etc., as compared to existing trusted approaches.

Figure 6 presents the utility value of each device during the communication process in the network. Such utility value is determined by converting the criteria's value from -1 to -I through the equations defined earlier. The presented figure shows the overall utility values of communicating device in the network. The devices having a high utility value are considered as highly trusted and recommended for decision-making in the network. In particular, our SMART approach is used to compute the utility value of each device, representing an efficient and accurate decision-making process compared to existing mechanisms.

Figure 7 represents the accuracy graph while recognizing the legitimate number of devices in the network accurately.

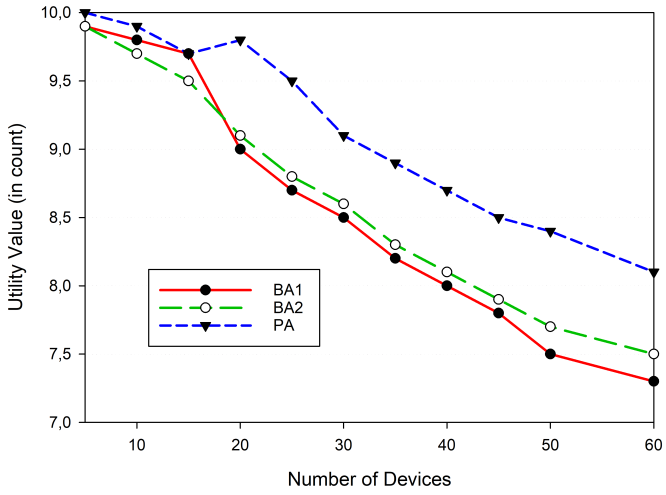

Fig. 6. Utility Value.

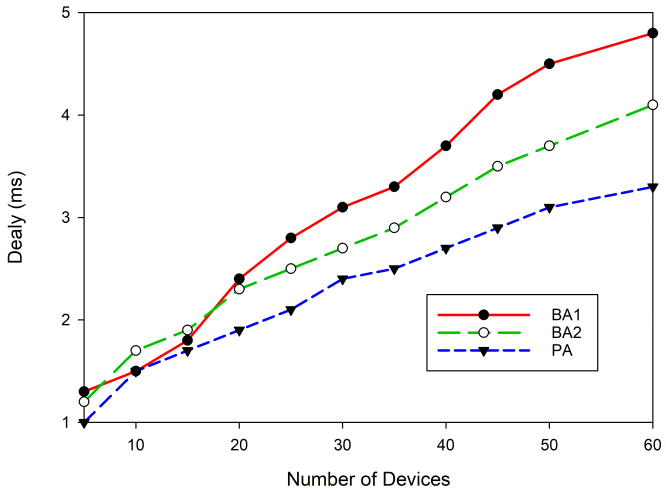

Fig. 8. Delay.

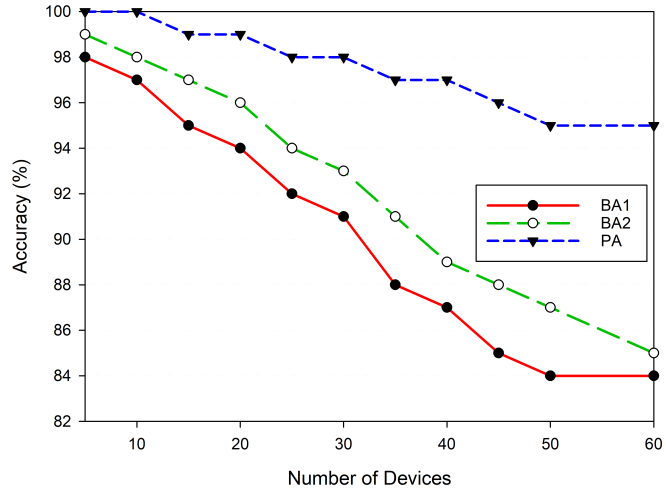

Fig. 7. Accuracy.

For this analysis, we have intentionally inserted a 20% of malicious devices in the network, and the proposed approach identifies the legitimate devices accurately because of the subjective recommendation approach that computes the device's trust and monitor their communication process in the network.

The general definition of delay means the amount of time required to reach one packet from source to its respective destination. Here the delay is computing based upon the decision asking process requested and proceed by the device upon analysing the change in network behaviour's. Finally, Figure 8 shows the delay involved for legitimate devices to take decisions upon request from their surrounding elements. The proposed mechanism presents the delay while making the decision by the devices during the communication process in the network. The proposed mechanism presents less delay while offering more accurate decisions as compared to existing schemes.

V. Conclusion and Future Work

The adoption of modern technologies like remote sensing has a major role in the smart cities' development. Yet, the adoption of various heterogeneous techniques may also open the door for intruders to compromise the connected devices, and control their functionalities. In this paper we proposed an integrated security mechanism to remotely sense the urban areas that are using IoT devices. The proposed mechanism involves two trust-establishment solutions for ensuring a secure communication network. Simulation results were carried-out using different metrics, and we compare against different state-of-art solutions; the obtained results evidence the high performance of our proposal in terms of utility value, accuracy, replay attack, satisfaction ratio and delay. The proposed mechanism provides approximate 97% improvement when compared to existing approaches for various security metrics.

As future work, we plan to investigate the case of AI-empowered adversary models, and improve our proposal to face these new kinds of attacks.

Acknowledgements

This work has been partially funded by R&D project PID2021-122580NB-100, from MCIN/AEI/10.13039/501100011033 and "ERDF A way of making Europe".

References

[1] T. Yigitcanlar, S. Teriman, Rethinking sustainable urban development: towards an integrated planning and development process, International Journal of Environmental Science and Technology 12 (1) (2015) 341–352.

[2] H. Ahvenniemi, A. Huovila, I. Pinto-Seppä, M. Airaksinen, What are the differences between sustainable and smart cities?, Cities 60 (2017) 234–245.

[3] M. Savastano, M.-C. Suciu, I. Gorelova, G.-A. Stativă, How smart is mobility in smart cities? an analysis of citizens' value perceptions through ict applications, Cities 132 (2023) 104071.

[4] H. Hu, J. Xu, M. Liu, M. K. Lim, Vaccine supply chain management: An intelligent system utilizing blockchain, iot and machine learning, Journal of Business Research 156 (2023) 113480.

[5] S. S. Joudar, A. Albahri, R. A. Hamid, Intelligent triage method for early diagnosis autism spectrum disorder (asd) based on integrated fuzzy multi-criteria decision-making methods, Informatics in Medicine Unlocked 36 (2023) 101131.
[6] G. Rathee, A. Kumar, C. A. Kerrache, A blockchain trusted mechanism (btm) for internet of unmanned things (iout) using comprehensive and adaptive schemes, in: Internet of Unmanned Things (IoUT) and Mission-based Networking, Springer, 2023, pp. 57–70.
[7] Y. Sahraoui, A. Korichi, C. A. Kerrache, M. Bilal, M. Amadeo, Remote sensing to control respiratory viral diseases outbreaks using internet of vehicles, Transactions on Emerging Telecommunications Technologies 33 (10) (2022) e4118.
[8] H. Shirmard, E. Farahbakhsh, R. D. Müller, R. Chandra, A review of machine learning in processing remote sensing data for mineral exploration, Remote Sensing of Environment 268 (2022) 112750.
[9] M. Nagy, G. Lăzăroiu, Computer vision algorithms, remote sensing data fusion techniques, and mapping and navigation tools in the industry 4.0-based slovak automotive sector, Mathematics 10 (19) (2022) 3543.
[10] N. C. Coops, P. Tompalski, T. R. Goodbody, A. Achim, C. Mulverhill, Framework for near real-time forest inventory using multi source remote sensing data, Forestry 96 (1) (2023) 1–19.
[11] O. Bello, S. Zeadally, Intelligent device-to-device communication in the internet of things, IEEE Systems Journal 10 (3) (2014) 1172–1182.
[12] X. Zheng, F. Zhang, K. Wang, W. Zhang, Y. Li, Y. Sun, X. Sun, C. Li, B. Dong, L. Wang, et al., Smart biosensors and intelligent devices for salivary biomarker detection, TrAC Trends in Analytical Chemistry 140 (2021) 116281.
[13] A. Singh, K. Chatterjee, Cloud security issues and challenges: A survey, Journal of Network and Computer Applications 79 (2017) 88–115.
[14] W. Ahmad, A. Rasool, A. R. Javed, T. Baker, Z. Jalil, Cyber security in iot-based cloud computing: A comprehensive survey, Electronics 11 (1) (2022) 16.
[15] T. Yoshizawa, D. Singelée, J. T. Muehlberg, S. Delbruel, A. Taherkordi, D. Hughes, B. Preneel, A survey of security and privacy issues in v2x communication systems, ACM Computing Surveys 55 (9) (2023) 1–36.
[16] H. Xia, Z. Li, Y. Zheng, A. Liu, Y.-J. Choi, H. Sekiya, A novel light-weight subjective trust inference framework in manets, IEEE Transactions on Sustainable Computing 5 (2) (2018) 236–248.
[17] S.-Y. Chou, Y.-H. Chang, A decision support system for supplier selection based on a strategy-aligned fuzzy smart approach, Expert systems with applications 34 (4) (2008) 2241–2253.
[18] T. Manoj, K. Makkithaya, V. Narendra, A trusted iot data sharing and secure oracle based access for agricultural production risk management, Computers and Electronics in Agriculture 204 (2023) 107544.
[19] P. Srividya, L. N. Devi, A. N. Rao, A trusted effective approach for forecasting the failure of data link and intrusion in wireless sensor networks, Theoretical Computer Science 941 (2023) 1–13.
[20] N. Yaakob, M. Almashor, A. F. M. Ahmed, Cost effective iot-based remote healthcare monitoring system for developing countries, in: 2021 IEEE International Conference on Smart Internet of Things (SmartIoT), IEEE, 2021, pp. 13–20.
[21] M. A. Simplicio, L. H. Iwaya, B. M. Barros, T. C. Carvalho, M. Näslund, Secourhealth: a delay-tolerant security framework for mobile health data collection, IEEE journal of biomedical and health informatics 19 (2) (2014) 761–772.
[22] A. Rahman, S. Roy, M. S. Kaiser, M. S. Islam, A lightweight multi-tier s-mqtt framework to secure communication between low-end iot nodes, in: 2018 5th International Conference on Networking, Systems and Security (NSysS), IEEE, 2018, pp. 1–6.
[23] S. Liu, L. Peng, T. Chi, X. Wang, Research on multi-source heterogeneous data collection for the smart city public information platform, in: 2016 IEEE International Geoscience and Remote Sensing Symposium (IGARSS), IEEE, 2016, pp. 623–626.
[24] T. S. Brisimi, S. Ariafar, Y. Zhang, C. G. Cassandras, I. C. Paschalidis, Sensing and classifying roadway obstacles: The street bump anomaly detection and decision support system, in: 2015 IEEE International Conference on Automation Science and Engineering (CASE), IEEE, 2015, pp. 1288–1293.
[25] L. Chen, Framework of sustainable urban spatial development model based on smart cities, in: 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS), IEEE, 2021, pp. 1823–1826.
[26] M. Lesani, N. Montazeri, Fuzzy trust aggregation and personalized trust inference in virtual social networks, Computational Intelligence 25 (2) (2009) 51–83.