Improving Big Data Clustering for Jamming Detection in Smart Mobility

Hind Bangui, Mouzhi Ge, Barbora Buhnova

Improving Big Data Clustering for Jamming Detection in Smart Mobility

Hind Bangui, Mouzhi Ge, and Barbora Buhnova

Faculty of Informatics, Masaryk University, Brno, Czech Republic
hind.bangui@mail.muni.cz, mouzhi.ge@muni.cz, buhnova@fi.muni.cz

Abstract. Smart mobility, with its urban transportation services ranging from real-time traffic control to cooperative vehicle infrastructure systems, is becoming increasingly critical in smart cities. These smart mobility services thus need to be very well protected against a variety of security threats, such as intrusion, jamming, and Sybil attacks. One of the frequently cited attacks in smart mobility is the jamming attack. In order to detect the jamming attacks, different anti-jamming applications have been developed to reduce the impact of malicious jamming attacks. One important step in anti-jamming detection is to cluster the vehicular data. However, it is usually very time-consuming to detect the jamming attacks that may affect the safety of roads and vehicle communication in real-time. Therefore, this paper proposes an efficient big data clustering model, coresets-based clustering, to support the real-time detection of jamming attacks. We validate the model efficiency and applicability in the context of a typical smart mobility system: Vehicular Ad-hoc Network, known as VANET.

Keywords: Smart mobility· Jamming attack· Anti-jamming· Big data clustering· VANET · Smart city

1 Introduction

Nowadays, smart mobility has become a critical transportation infrastructure [39,9] in smart cities as it provides a variety of mobility services, such as relieving the traffic congestion in cities and providing better access to public transport. In [1], smart mobility is described as: "The use of ICT in modern transport technologies to improve urban traffic". Likewise, in [43], it is defined as: "local and supra-local accessibility, availability of ICTs, modern, sustainable and safe transport systems". Thus, smart mobility can be considered as a management strategy that produces decisions based on the collected data [9,31] from vehicle-to-anything communications, such as vehicle-to-vehicle, vehicle-to-infrastructure, vehicle-to-pedestrian, and infrastructure-to-pedestrian [44]. For instance, a road infrastructure monitoring system uses e-bikes proposed in [25] to support municipal transportation activities. Further, an image processing application based on deep learning has been integrated into e-bikes to facilitate the detection of road anomalies such as litter and damage of roads. It can be

seen that smart mobility is a fruitful domain that integrates different up-to-date techniques such as the autonomous driving Internet of Things (IoT) and machine learning. In [21], a vehicular interface notation has been developed to help older customers of smart vehicles to control their driving experience better and improve their cognitive ability. Similarly, in [41], a machine learning system has been proposed to exploit data from autonomous vehicles and external IoT data sources to predict pedestrian's next movement steps using real-time trajectory. The suggested solution ensures safety in urban environments by enhancing autonomous driving efficiently in local public transport services. The recent works indicate that smart mobility is driven by data-intensive processes focused on managing people's mobility and personalizing transport solutions according to the specific needs of cities [8]. On the other hand, smart mobility advances the transport services and quality of citizens' life in smart cities [17,29,16].

Enabling smart mobility in urban environments is, however, challenging because attackers are attempting to access or tamper with valuable mobility data (e.g., personal user information) or disrupt network communication. Since smart mobility generates a massive amount of data, such as sensor data on the road or vehicle communication data, various security applications make use of big data analytics to secure smart mobility applications. There are different prevalent attacks in the smart mobility domain. One of the frequently cited ones is the jamming attack. Jamming attacks can severely influence road safety and vehicle communications.

In order to detect the jamming attacks in smart mobility, different anti-jamming applications have been proposed, which , however, suffer from the inefficiency of the data clustering during the jamming attack detection. In this paper, we, therefore, propose a solution to support the real-time detection of jamming attacks via efficient big data clustering of vehicular data. The solution is mainly based on the coresets technique and Vehicular Ad-hoc Network (VANET) is used as a practical scenario of smart mobility [5,10], where we consider particularly the application of clustering algorithms in anti-jamming detection solutions designed for securing VANET communications.

The remainder of the paper is organized as follows. Section 2 is dedicated to understanding the vulnerability of smart mobility systems by using VANET as an example of smart mobility applications. Then in Section 3, we provide an overview of related work concerning anti-jamming applications based on clustering techniques. In Section 4, we present a solution that aims at increasing efficiency the clustering process while keeping the quality of analytics. In section 5, we conduct an experiment to show the benefits of the proposed solution. Finally, Section 6 concludes the paper and outlines future research.

2 Security in Smart Mobility

Smart mobility intends to control the behavior of smart devices in urban environments by collecting, sharing, and utilizing trace data. Vehicular Ad-hoc Network (VANET) is a typical smart mobility system that can be used to share data

within vehicle-to-anything communication. For example, VANET applications such as smart cars are used to support the safety of traffic flows [35,20,40]. The vehicles exchange messages with neighboring vehicles (members of a VANET) and with RSUs (roadside units) to inform them about e.g. their location and speed, and get traffic conditions of the road. However, a malicious attacker may remotely access a target vehicle, possibly tampering with the behavior of the vehicle, such as misinforming the driver.

Constant jamming is one type of jamming attacks that is considered as a severe threat to VANET security [22,40]. In this attack, a jammer regularly sends repeated signals to interfere with the communication between vehicles in the affected network area, where the target vehicles think that the state of the channel is still busy. Consequently, they cannot send or receive packets that can be carrying important information, such as weather and accidents. In other words, when jamming occurs, the sender may send packets. However, the receiver might not be able to receive all the packets sent by the sender. Thus, the failure of receiving or disseminating these packets can lead to the insufficiency of the VANET. Smart mobility systems require the optimized use of detection attack applications to cope with the security and privacy threats.

Several detection attack systems are proposed in the previous literature [19,40]. Table 1 presents a list of typical attacks in smart mobility. However, developing security and privacy solutions is more challenging in smart mobility infrastructure as data are subject to several malicious attacks causing wrong outcomes (i.e., wrong traffic). Especially, the big data clustering technique is used to facilitate the attack detection. Thus, we focus on examining how big data clustering algorithms in smart mobility [5,10] are investigated to deal with vulnerable attacks. Particularly, it is valuable to study the clustering for detection applications that deal with jamming attacks caused several damages, such as disruption of car-to-car communications.

3 Clustering for Anti-Jamming Detection

The concept of big data clustering is very important in smart mobility since it contributes to improving the sustainability, scalability, and reliability of smart mobility systems [5], such as associating mobile nodes into groups, ensuring the stability of channel access management, traffic safety, and QoS Assurance. Many jamming detection approaches in VANET have exploited the advantages of clustering algorithms by collecting jamming measurements and then accurately grouping them into the cluster [6,32]. For example, in [15], a novel jamming detection framework was proposed to detect the presence of a jammer in hierarchical cluster-based wireless sensor networks. The proposed anti-jamming detection method also exploits the benefits of the unsupervised hierarchical algorithm for achieving energy efficiency by re-clustering, overcoming network issues (i.e., reducing the communication overhead), decreasing collision, and improving throughput. Similarly, in [23], a jamming detection solution was developed by leveraging the K-means algorithm, which is one of the most commonly used

Table 1. Cyber attacks in smart mobility

Cyber attacks	Description
Intrusion	Aim at analyzing vehicular data to inspect the abnormal behavior in VANET under different scenarios, and then generate an alarm filtering technique for any detected security anomaly.
Misbehavior	Aim at analyzing the behavior of vehicles to detect malicious node that may send incorrect information to other vehicles, and then cause malfunctioning VANET applications.
DDoS	Eliminate the DDoS attacks that make the network services unavailable from different locations.
Jamming	Eliminate jamming attacks that make physical resources unavailable by interfering with the radio frequencies used by VANET vehicles.
Sybil	Aim at detecting the Sybil vehicle attack that can forge different false identities, where each pseudonym acts as a virtual vehicle.

partitioned clustering algorithms in Big Data Analytics. This work reflects the benefits of using clustering algorithms in VANETs, where the advantages of k-means are used to differentiate intentional cases from unintentional jamming.

The collected jamming measurements are grouped into the interference cluster accurately, and then the specific characteristics of each attack are extracted. Thus, the unsupervised method is aimed at determining whether jamming occurs due to a malicious jammer or whether it is caused unintentionally. Consequently, if jamming is correctly identified as interference, vehicles can preserve their communications either by changing their channel or by temporarily altering their route. Likewise, in [4], a multi-cluster localization (M-cluster) algorithm and an x-rayed jammed-area localization (X-ray) algorithm were successively developed based on fuzzy c-means and K-means to deal with the multi-jammer localization problem in WSNs, which could launch collaborative attacks. In [34], the advantages of K-means were used to predict the number of multiple jamming attackers and ensure the preset functions of VANET. In [33], an anti-jamming method based on fuzzy c-means was proposed to determine the localization and number of jamming attackers. Accordingly, the cluster analysis process simplifies data manipulation by finding similar structures in the data and classifying each object according to its nature. As a result, vehicles can adequately avoid malicious jamming attacks, decrease their collisions, and preserve their communications [30,27,28].

Nevertheless, the existing anti-jamming solutions suffer from efficiency issues due to the growth of smart mobility data and it is time-consuming to perform a computational clustering process.

Furthermore, vehicles in the smart mobility context are producing big data at a rapid rate in the dynamic urban environment. Thus, the time and cost of

Table 2. Overview of anti-jamming applications based on Clustering algorithms

Papers	Description	Clustering algorithms used
[23]	Study jamming attack detection in a pair of RF (radio frequency) communicating vehicles.	K-means
[26]	Ensure secure communication and defend RF jamming attacks.	K-Nearest Neighbors and Random Forests
[15]	Detect jamming attacks.	Hierarchical clustering
[6]	Predict jamming attacks.	Clusters
[32]	Detect jamming attacks.	Clusters
[4]	Detect multi-jammer localization attacks.	Fuzzy c-Means, k-means
[34]	Estimate the number of multiple jamming attackers.	K-means
[33]	Detect the localization of multiple jamming attackers in VANET.	Fuzzy c-Means

the clustering process will increase since they depend on the volume of datasets, which is definitely difficult to be handled in real-time. Yet, the study of data prioritization is required since it aims at serving the real-time Big Data Analytics by selecting the most valuable data from the initial input data [7]. As a result, the anti-jamming applications can detect in real-time viral attacks that cause smart mobility system failures.

4 Coresets-based Anti-Jamming Detection

In this section, we propose a model that aims at minimizing the response time of anti-jamming detection by accelerating the clustering process. Figure 1 presents a general process of attack detection based on the application of data clustering, where a predefined list of features is extracted from vehicular data to detect the characteristics of jamming attacks. The selection of features is according to the context of the proposed anti-jamming solutions, for example, GPS information is used to recognize cases of intentional jamming [33]. After that, the clustering method can be used to analyze vehicular data and classify timely the malicious nodes from benign ones. The coresets can be used to accelerate clustering the big mobility data. In the context of jamming detection, the anti-jamming application is able to deal with the specific characteristics of each jamming attack timely and effectively.

4.1 Coresets

The idea of using approximated data has been investigated in sensor networks [14,12], where coresets are used to extract small data samples that represent

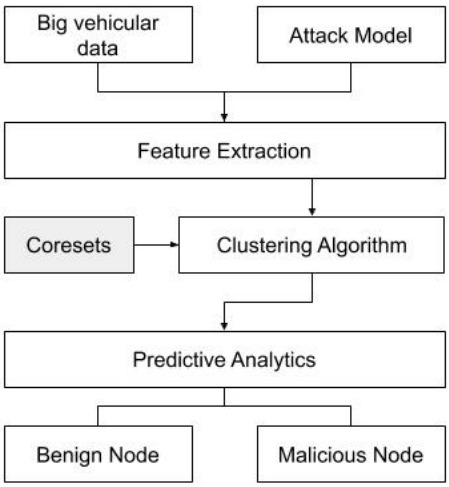

Fig. 1. Coresets-based predictive analytics for attacks in smart mobility

the original data approximately, and then solve compression issues of trajectory data in road networks [12,13,14], such as improving the run-time performance of location-based applications. Moreover, coresets not only can reduce the data scale while keeping the original data distribution [11,24], but also can be used for improving the quality of clustering [18,37]. For Example, ProTraS [38] is a coreset construction algorithm that aims at generating a data sample to deal with big data clustering problems [3,2]. The main idea of ProTraS is to select a representative point based on a probability of cost reduction. Given an $\epsilon > 0$, for each iteration of the algorithm, it adds a new representative into a group of the sample with the highest probability of the cost reduction. When the cost drops below a threshold, which depends on ϵ, the algorithm stops. The algorithm finds the nearest group for points that are not yet assigned to any group of the current sample. The point among them is determined to be the new representative if it is farthest in its group and has the highest probability. That means, the representative selected by ProTraS is the farthest-first traversal item of a given group. As a result, this coreset construction algorithm leads to enhancing the quality of clusters that are required for ensuring the accuracy of the Big Data Analytics outcomes [3,2].

In this work, we aim to investigate the advantages of coresets to optimize the quality of clustering used in anti-jamming detection. Particularly, we use coresets method to deal with the clustering formulation and complexity. We have referred to the coresets technique discussed in [42]. This is an improvement version of the ProTraS algorithm [38] by using a post-processing task. Given a dataset $P = \{x_i\}$, for $i = 1, 2, \ldots, n$ and a given $\epsilon > 0$, the method firstly calls ProTraS to obtain $S = \{y_j\}$ and $P(y_j)$ for $j = 1, 2, \ldots, s$. The method next tries to find some sample points that have low representativeness and remove them

from the sample. A point in remaining points is then replicated by the center of the set of patterns which the point represents. The details of the method are given in Algorithm 1.

Algorithm 1 Coresets-based algorithm for sampling [42]

Require: $P = \{x_i\}$, for $i = 1, 2, \ldots, n$, a tolerance $\epsilon > 0$.
Ensure: A sample $S = \{y_j\}$ and $P(y_j)$, for $j = 1, 2, \ldots, s$.

1: Call ProTraS for P and ϵ to obtain $S = \{y_j\}$ and $P(y_j)$.
2: $S' = \emptyset$.
3: **for all** $y_j \in S$ **do**
4: **if** $|P(y_j)|$ is greater than a threshold **then**
5: $y_k^* = \arg\min_{y_k \in P(y_j)} \sum_{y_l \in P(y_j)} d(y_k, y_l)$.
6: $S' = S' \cup \{y_k^*\}$.
7: **end if**
8: **end for**
9: $S = S'$.
10: **return** S and $P(y_j^*)$, for $j = 1, 2, \ldots, s'$, where $s' \leq s$.

Line 4 determines which sample points will be select into our sample S'. This is performed using a threshold. $|P(y_j)|$ denotes the number of patterns in P with $y_j \in S$ being their representative. A small value of $|P(y_j)|$ means that the representativeness of y_j is low. Accordingly, it is removed from the sample. The value of the threshold should be chosen due to the distribution characteristics of datasets. For $y_j \in S$ that is not removed, line 5 computes the center of the group represented by y_j, to consider replacing it. The center here, denoted by y_k^*, is defined to be the point in $P(y_j)$ such that the total distance to all others in the group is minimized. The set S' including such y_k^* is the output sample of the algorithm.

5 Experiment Evaluation

In the experiment, we focus on examining how the integration of the coreset method [42] can facilitate the analysis process of anti-jamming applications. To do that, we study vehicular data clustering. Then, we present the details of clustering quality evaluation.

5.1 Experimental Setting

The goal of this experiment is to detect the presence of a constant jamming attack. This latter is detected by monitoring the signal power that is reported via the Received Signal Strength Indicator (RSSI), which is an expression of the SNIR (Signal-to-Noise-and-Interference Ratio). In the presence of the malicious attack, the probability of successful message reception is decreased as well as

SNIR is decreased too. For achieving this experiment, we have initially referred to a study in [36] that has explored the impact of different jamming attacks, including a constant jamming case, in VANETs. Then, we have selected its dataset [1] that contains traces of 802.11p packets with and without the presence of constant jamming signals.

Table 3 presents the network configuration used for creating a series of constant jamming scenarios. The number of generated packets is 25,000. The vehicular network features used in this experiment are as follows: Node-Id-number, type, vehicle position, GPS-time, speed, time sender, time receiver, RSSI, SNIR, and vehicle heading. For storage and clusters, we used the permanent cloud environment offered by MetaCentrum[2].

Table 3. Experimental parameters

Linkbird	Data Rate	6 Mbps
	Transmit power	17.48 dBm
	Payload length	100 Byte
	Packet generation rate	100 $packets/s$
Constant jamming	Transmit power	16.75 dBm
	Signal duration	64 μs
	Signal preparation time	10 μs
General	Center frequency	5.875 GHz

5.2 Clustering Quality Measurement

Our goal in this experiment is to evaluate the representation of clustering sampling yielded from K-means and its improved versions, which are: K-means++ and Fuzzy c-means. We selected k-means as our clustering algorithm, as k-means is a widely used and efficient unsupervised algorithm that uses an iterative method to divide a given dataset into several clusters noted as k. Next, the produced clusters are positioned as points, and all samples are linked with the nearest cluster and adjusted; then, the process overuses the new adjustments until the desired result is achieved. Thus, this algorithm is easy to implement, efficient in terms of its computational costs, and offers easily interpretable clustering results.

On the other hand, since K-means is sensitive to initialization, it is sensitive to the presence of outliers because the "mean" is not a robust statistic value. Therefore, k-means may yield poor outcomes and take more processing time. For that reason, we have evaluated the quality of the obtained clusters both with and without the application of the coresets method. We used the improved versions of K-means (i.e., fuzzy c-means) to evaluate how coresets could influence the

[1] `https://crawdad.org/keyword-vehicular-network.html`
[2] `https://www.cerit-sc.cz`

quality of the clusters by using a list of metrics. For instance, the Dunn index (DI) is used as an internal evaluation metric to determine how well each sample lies within its cluster. A higher DI indicates better clustering. Likewise, we used a second internal metric, named the Davies–Bouldin index (DBI), to evaluate how well the clustering has been done by using the quantities and features inherent to the selected database. A lower DBI indicates better clustering.

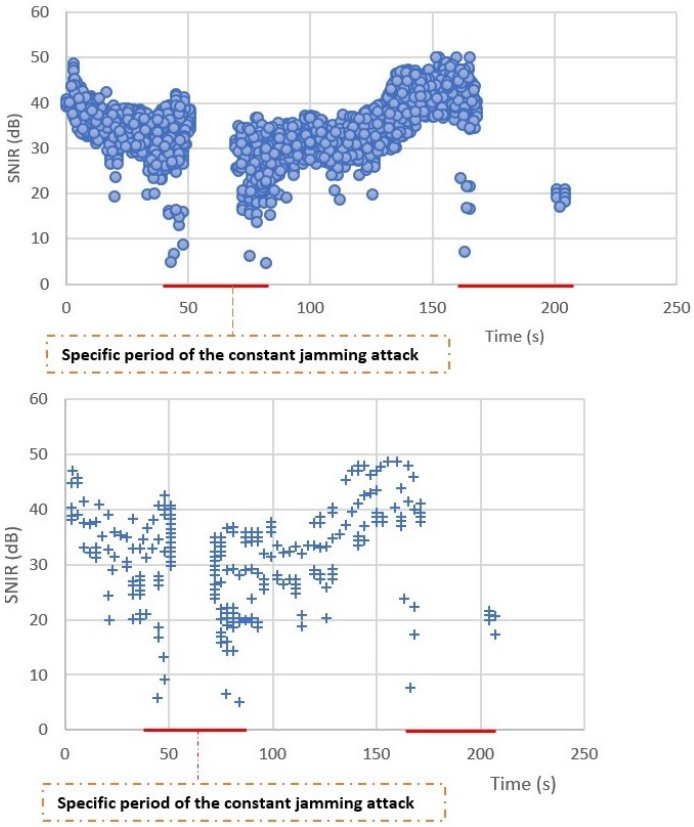

Fig. 2. Before and after using coresets, Sample size = 25,000 and Sample size = 479

5.3 Experimental Results

Figure 2 represented the mapping of the SNIR time evolution. One can see that the sample size is reduced from 25,000 to 479 due to the application of the coreset. Consequently, the time analysis process is also reduced. Thus, the combination of the coresets with clustering algorithms could help the anti-jamming applications to learn quickly from the approximated data that represent the original data

source. As a result, they can detect the presence of constant jamming attacks rapidly.

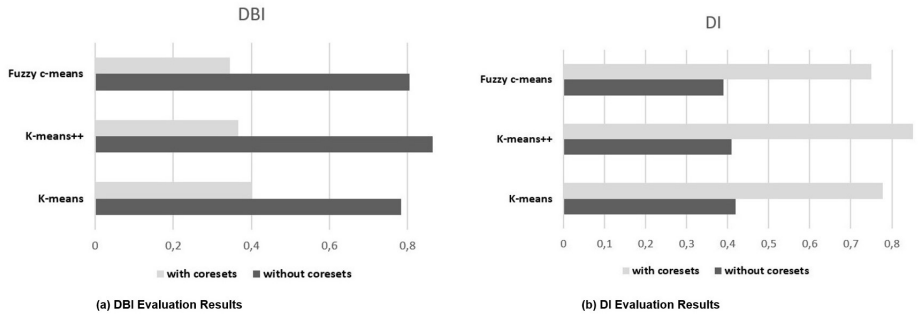

Fig. 3. Clustering Evaluation Results based on DBI and DI metrics

Meanwhile, the results of internal and external cluster validity indices in Figure 3 showed that the application of k-means, k-means++, and Fuzzy c-means based on coresets provides promising results compared to their regular application. DBI (Figure 3 a) and DI (Figure 3 b) achieved better values with the coresets compared to the original application of clustering algorithms. Further, DBI and DI reflect how well each sample lies within its cluster. Accordingly, the integration of the coresets with k-means and its improved versions increases the quality of clusters. Besides, K-means shows better efficiency than k-means++ and Fuzzy c-means in term of time. However, we noticed that the application of the coresets supports Fuzzy c-means to proceed quickly compared to its regular time process. Thus, the proposed solution keeps and even significantly improves the quality of the clusters in terms of DBI and DI measurements.

From Figure 4, one can see that the time of the clustering process is improved on average 132 times across k-means, k-means++, and Fuzzy c-means. Furthermore, all the clustering time is within 1 second, which indicates that the solution can facilitate real-time jamming detection in VANET. In other words, the anti-jamming applications can detect the presence of the viral constant jamming attack and cope with it in real-time, which is a good starting point not only for enhancing the security mechanisms adopted by anti-jamming applications but also for supporting the other detection attack systems based-clustering that have to deal with viral attacks in real-time.

On the other side, the experiment results could be a big motivation for further use of approximated data in smart mobility systems not only for avoiding (or minimizing) the negative impact of malicious attacks, such as damage of personal properties (i.e., cars) and sharing wrong traffic information, but also for supporting the progress of smart mobility applications in urban environments.

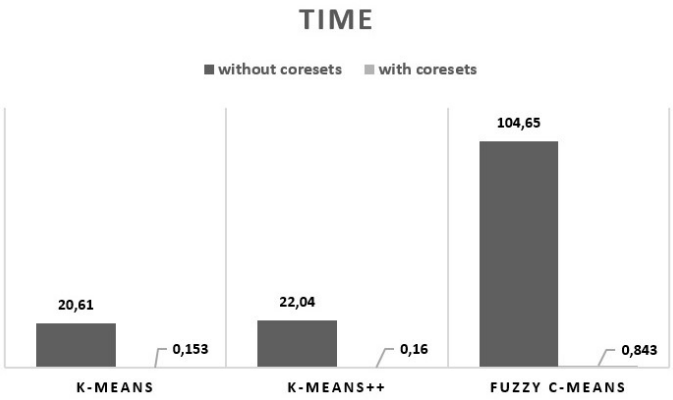

Fig. 4. Comparison of clustering processing time (in seconds)

6 Conclusions

In this paper, we have proposed a model based on the coresets techniques to address the real-time jamming attack detection in smart mobility. Our model demonstrates how to process the big mobility data and use clustering techniques in anti-jamming applications. In order to validate the proposed model, we have conducted an experiment in the VANET setting and our results have shown that the proposed solution can significantly increase the detection efficiency of anti-jamming applications while keeping the clustering quality. With the significant decrease in clustering time, the proposed solution enables the anti-jamming applications to perform real-time jamming detection in smart mobility. Furthermore, our model can also be easily integrated into different smart mobility systems and used to advance the efficiency of other big data applications in the Internet of Vehicles.

As future work, we plan to conduct more experiments with other clustering algorithms, and extend the coresets to detect and discoverer other attacks in smart mobility. Furthermore, we plan to deploy our solution in different real-world scenarios such as the Internet of Vehicles and benchmark the performance of the proposed solution.

Acknowledgements

The work was supported from ERDF/ESF "CyberSecurity, CyberCrime and Critical Information Infrastructures Center of Excellence" (No. CZ.02.1.01/0.0/0.0 /16_019/0000822).

References

1. Albino, V., Berardi, U., Dangelico, R.M.: Smart cities: Definitions, dimensions, performance, and initiatives. Journal of urban technology **22**(1), 3–21 (2015)
2. Bangui, H., Ge, M., Buhnova, B.: Exploring big data clustering algorithms for internet of things applications. In: IoTBDS. pp. 269–276 (2018)
3. Bangui, H., Ge, M., Buhnova, B.: A research roadmap of big data clustering algorithms for future internet of things. International Journal of Organizational and Collective Intelligence **9**(2), 16–30 (2019)
4. Cheng, T., Li, P., Zhu, S., Torrieri, D.: M-cluster and x-ray: Two methods for multi-jammer localization in wireless sensor networks. Integrated Computer-Aided Engineering **21**(1), 19–34 (2014)
5. Cooper, C., Franklin, D., Ros, M., Safaei, F., Abolhasan, M.: A comparative survey of vanet clustering techniques. IEEE Communications Surveys & Tutorials **19**(1), 657–681 (2016)
6. Cordero, C.V., Lisser, A.: Jamming attacks reliable prevention in a clustered wireless sensor network. Wireless Personal Communications **85**(3), 925–936 (2015)
7. Darwish, T.S., Bakar, K.A.: Fog based intelligent transportation big data analytics in the internet of vehicles environment: motivations, architecture, challenges, and critical issues. IEEE Access **6**, 15679–15701 (2018)
8. Del Vecchio, P., Secundo, G., Maruccia, Y., Passiante, G.: A system dynamic approach for the smart mobility of people: Implications in the age of big data. Technological Forecasting and Social Change **149**, 119771 (2019)
9. El-Din, D.M., Hassanien, A.E., Hassanien, E.E.: Information integrity for multi-sensors data fusion in smart mobility. In: Toward Social Internet of Things (SIoT): Enabling Technologies, Architectures and Applications, pp. 99–121. Springer (2020)
10. Elhoseny, M., Shankar, K.: Energy efficient optimal routing for communication in vanets via clustering model. In: Emerging Technologies for Connected Internet of Vehicles and Intelligent Transportation System Networks, pp. 1–14. Springer (2020)
11. Feldman, D., Schmidt, M., Sohler, C.: Turning big data into tiny data: Constant-size coresets for k-means, pca and projective clustering. In: Proceedings of the twenty-fourth annual ACM-SIAM symposium on Discrete algorithms. pp. 1434–1453. Society for Industrial and Applied Mathematics (2013)
12. Feldman, D., Sugaya, A., Rus, D.: An effective coreset compression algorithm for large scale sensor networks. In: 2012 ACM/IEEE 11th International Conference on Information Processing in Sensor Networks (IPSN). pp. 257–268. IEEE (2012)
13. Feldman, D., Sung, C., Rus, D.: The single pixel gps: learning big data signals from tiny coresets. In: Proceedings of the 20th International Conference on Advances in Geographic Information Systems. pp. 23–32. ACM (2012)
14. Feldman, D., Xiang, C., Zhu, R., Rus, D.: Coresets for differentially private k-means clustering and applications to privacy in mobile sensor networks. In: 2017 16th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN). pp. 3–16. IEEE (2017)
15. Ganeshkumar, P., Vijayakumar, K., Anandaraj, M.: A novel jammer detection framework for cluster-based wireless sensor networks. EURASIP Journal on Wireless Communications and Networking **2016**(1), 35 (2016)
16. Ge, M., Bangui, H., Buhnova, B.: Big data for internet of things: A survey. Future Generation Computer Systems **87**, 601–614 (2018)

17. Han, J.H., Shin, Y.S., Lee, S.H.: Smart mobility creating smart space: 3d smart aquarium bus. In: 2019 IEEE Transportation Electrification Conference and Expo. pp. 1–5. IEEE (2019)
18. Har-Peled, S., Mazumdar, S.: On coresets for k-means and k-median clustering. In: Proceedings of the Thirty-sixth Annual ACM Symposium on Theory of Computing. pp. 291–300. STOC '04, ACM, New York, NY, USA (2004). https://doi.org/10.1145/1007352.1007400, http://doi.acm.org/10.1145/1007352.1007400
19. Hasrouny, H., Samhat, A.E., Bassil, C., Laouiti, A.: Vanet security challenges and solutions: A survey. Vehicular Communications **7**, 7–20 (2017)
20. Hernafi, Y., Ahmed, M.B., Bouhorma, M.: Smart mobility and driver behavior correlated with vehicular networks under a social perception in smart cities. International Journal of Information Science and Technology **2**(2), 35–47 (2019)
21. Ikem, C.: Users as programmers: Developing a vehicular interface notation for older users of smart vehicles. In: Proceedings of the 1st ACM Workshop on Emerging Smart Technologies and Infrastructures for Smart Mobility and Sustainability. pp. 15–19. ACM (2019)
22. Kalkundri, R.U., Khanai, R., Praveen, K.: Survey on security for wsn based vanet using ecc. International Annals of Science **8**(1), 30–37 (2020)
23. Karagiannis, D., Argyriou, A.: Jamming attack detection in a pair of rf communicating vehicles using unsupervised machine learning. Vehicular Communications **13**, 56–63 (2018)
24. Karmakar, B., Das, S., Bhattacharya, S., Sarkar, R., Mukhopadhyay, I.: Tight clustering for large datasets with an application to gene expression data. Scientific reports **9**(1), 3053 (2019)
25. Katto, J., Takeuchi, M., Kanai, K., Sun, H.: Road infrastructure monitoring system using e-bikes and its extensions for smart community. In: Proceedings of the 1st ACM Workshop on Emerging Smart Technologies and Infrastructures for Smart Mobility and Sustainability. pp. 43–44. ACM (2019)
26. Kosmanos, D., Karagiannis, D., Argyriou, A., Lalis, S., Maglaras, L.: Rf jamming classification using relative speed estimation in vehicular wireless networks. arXiv preprint arXiv:1812.11886 (2018)
27. Liang, J., Chen, J., Zhu, Y., Yu, R.: A novel intrusion detection system for vehicular ad hoc networks (vanets) based on differences of traffic flow and position. Applied Soft Computing **75**, 712–727 (2019)
28. Liu, X., Xu, Y., Jia, L., Wu, Q., Anpalagan, A.: Anti-jamming communications using spectrum waterfall: A deep reinforcement learning approach. IEEE Communications Letters **22**(5), 998–1001 (2018)
29. Matos, A., Pinto, B., Barros, F., Martins, S., Martins, J., Au-Yong-Oliveira, M.: Smart cities and smart tourism: What future do they bring? In: World Conference on Information Systems and Technologies. pp. 358–370. Springer (2019)
30. Mokdad, L., Ben-Othman, J., Nguyen, A.T.: Djavan: Detecting jamming attacks in vehicle ad hoc networks. Performance Evaluation **87**, 47–59 (2015)
31. Ning, Z., Xia, F., Ullah, N., Kong, X., Hu, X.: Vehicular social networks: Enabling smart mobility. IEEE Communications Magazine **55**(5), 16–55 (2017)
32. Osanaiye, O., Alfa, A., Hancke, G.: A statistical approach to detect jamming attacks in wireless sensor networks. Sensors **18**(6), 1691 (2018)
33. Pang, L., Chen, X., Shi, Y., Xue, Z., Khatoun, R.: Localization of multiple jamming attackers in vehicular ad hoc network. International Journal of Distributed Sensor Networks **13**(8) (2017)

34. Pang, L., Guo, P., Chen, X., Li, J., Xue, Z.: Estimating the number of multiple jamming attackers in vehicular ad hoc network. In: 2017 6th International Conference on Computer Science and Network Technology (ICCSNT). pp. 366–370. IEEE (2017)
35. Pereira, J., Ricardo, L., Luís, M., Senna, C., Sargento, S.: Assessing the reliability of fog computing for smart mobility applications in vanets. Future Generation Computer Systems **94**, 317–332 (2019)
36. Punal, O., Pereira, C., Aguiar, A., Gross, J.: Experimental characterization and modeling of rf jamming attacks on vanets. IEEE transactions on vehicular technology **64**(2), 524–540 (2014)
37. Ros, F., Guillaume, S.: Protras: A probabilistic traversing sampling algorithm. Expert Systems with Applications **105**, 65–76 (2018)
38. Ros, F., Guillaume, S.: Protras: A probabilistic traversing sampling algorithm. Expert System with Applications **105**, 65–76 (2018). https://doi.org/10.1016/j.eswa.2018.03.052, `https://doi.org/10.1016/j.eswa.2018.03.052`
39. Šemanjski, I., Mandžuka, S., Gautama, S.: Smart mobility. In: 2018 International Symposium ELMAR. pp. 63–66. IEEE (2018)
40. Seuwou, P., Banissi, E., Ubakanma, G.: The future of mobility with connected and autonomous vehicles in smart cities. In: Digital Twin Technologies and Smart Cities, pp. 37–52. Springer (2020)
41. Solmaz, G., Berz, E.L., Dolatabadi, M.F., Aytaç, S., Fürst, J., Cheng, B., Ouden, J.d.: Learn from iot: pedestrian detection and intention prediction for autonomous driving. In: Proceedings of the 1st ACM Workshop on Emerging Smart Technologies and Infrastructures for Smart Mobility and Sustainability. pp. 27–32. ACM (2019)
42. Trang, L.H., Bangui, H., Ge, M., Buhnova, B.: Scaling big data applications in smart city with coresets. In: Proceedings of the 8th International Conference on Data Science, Technology and Applications. Prague, Czech Republic (2019)
43. Vanolo, A.: Smartmentality: The smart city as disciplinary strategy. Urban studies **51**(5), 883–898 (2014)
44. Zaffiro, G., Marone, G.: Smart mobility: new roles for telcos in the emergence of electric and autonomous vehicles. In: 2019 AEIT International Conference of Electrical and Electronic Technologies for Automotive (AEIT AUTOMOTIVE). pp. 1–5. IEEE (2019)