Journal of Engineering Sciences
Vol 11, Issue 4 ,April/2020
ISSN NO:0377-9254

ON THE EFFICIENCY OF VEHICULAR CONNECTIVITY PRIVACY METRICS

P. PHANINDRA KUMAR REDDY[1], S. MOUNIKA[2], K. ANUSHA[3]
[1]Assistant Professor, Dept of CSE, AITS, Rajampet, AP, India.
[2,3]Student, Dept of CSE, AITS, Rajampet, AP, India.

ABSTRACT- Vehicle connectivity plays a key role in the near-future transport of vehicles, offering features such as increased traffic safety and improvements to wireless technologies. Nonetheless, vehicle communication can disclose the positions of drivers and thus poses risks to privacy. Several mechanisms have been introduced to protect privacy in vehicle communication, and their efficacy is typically measured with data protection metrics. In this paper, we analyze and compare the strength of 41 privacy metrics in terms of four new criteria. We test all four criteria with state-of - the-art adversary models on real and virtual traffic and create a ranking of privacy metrics. Our results show that no single metric predominates over all parameters and traffic conditions.

Keywords- Anonymity, monotonicity, privacy metrics, technology that improves privacy, vehicle communications, vehicle networks.

I. INTRODUCTION

Vehicular communication technologies allow vehicles to communicate with other vehicles and infrastructure nodes so that features such as collision avoidance intersection and cooperative adaptive cruise control are possible. For these features to be realized, vehicles transmit sensitive data –often without encryption –such as their location, speed and heading. Anyone within the wireless transmission range can use this information to track vehicles and their drivers on a large scale, which raises concerns about privacy [8]. Such privacy issues are well understood, and many solutions to protecting privacy have been suggested. For example, vehicles are often assumed to have a pool of pseudonyms in addition to a long-term identifier, and different schemes have been proposed to change pseudonyms in a privacy-preserving way without compromising safety and accountability [30]. The data security metrics measure how effectively these systems are protecting privacy.

Contributes. We are making two contributions in this paper to research into privacy in vehicle networks.

First, we are contributing to the analytical basis of data protection calculation by proposing a framework for measuring the strength of data protection metrics using four novel criteria:

- Certain monotonicity requires metrics to display declining privacy with growing adversarial power. It prevents misjudging the effectiveness of new technologies for privacy enhancing (PETs).
- Extent allows metric values to be distributed across a wide range of values, and evenness requires a consistent distribution of metric values.
- Together, scale and evenness allow fine-grained analysis of privacy within a context, e.g. between cars, over time, and between parts of a city, as well as simulation of privacy rates.
- Shared value range means that when implemented in different traffic environments, metric values share a common value range. This makes comparisons between various scenarios.

Second, we assess the strength of 41 privacy metrics for vehicle networks, rate the metrics in the four parameters according to their ratings, and make specific recommendations for the use of data protection metrics in vehicle networks.

- In particular, our key findings and recommendations are: in all four measures, no single metric excels, and the intensity of many metrics varies between traffic conditions. So we always suggest using metrics packages that incorporate the strengths of different metrics.
- Many metrics have significant weaknesses that were used in the past to test pseudonym-changing systems, such as the mean tracking length, time / distance to

Journal of Engineering Sciences

uncertainty, and overall tracking time. And we recommend using these metrics with caution, if any.

II. RELATED WORK

In this paper, we draw on related work on data-protection and data-protection measures in vehicular communications, data-protection metrics in other fields, and studies on data-protection intensity assessments.

2.1 Vehicle network Privacy Metrics

In the past 15 years, many different privacy metrics have been proposed to evaluate the effectiveness of new PETs. In the vehicular networking context, privacy metrics have been used, for example, to evaluate new pseudonym-changing strategies.

Such techniques decide whether and how often vehicles alter their public broadcast identifiers to decrease the risk of being monitored by an adversary. Proposed strategies involve silent times, username swapping, and mixing zones, and in each case the privacy offered by each strategy was measured using data protection metric.

2.2 Criteria for data privacy

Many scholars have suggested standards that should follow good data privacy metrics. For example, they should be understandable and indicate the chances of success of the opponent; they should demonstrate both the level of privacy and the potential for breaches of privacy; they should include precision, ambiguity, and consistency as three components of the success of the opponent; and they should measure the amount of resources an opponent needs to succeed. In this paper, in addition to monotonicity, we suggest three novel criteria for determining the reliability of privacy metrics for vehicle networks.

2.3 Assessing data protection metrics

It is crucial to choose strong privacy metrics when assessing new PETs, since weak privacy metrics can overestimate privacy and lead to real-world violations of privacy. In this paper, we describe these consumer and adversary models for vehicle communications, extend the set of metrics examined to include metrics appropriate for vehicle communications, and add three new metric strength criteria: magnitude, evenness and shared range of values.

2.4 Visualisation of Privacy

Our analysis of the privacy metrics on city maps revealed that privacy also depends on a city's road layout and traffic density. A possible consequence for the design of PETs is that it may be prudent to apply one PET in city centers with dense traffic, and to choose another PET for suburbs with less dense traffic, or to change parameter settings to provide sufficient privacy in all areas.

III. METHODOLOGY

To apply our methodology (see Fig. 1), we first identify user and adversary situations in which the adversary is aimed at infering user behavior. Second, in each scenario we quantify the values of a set of privacy metrics and finally we assess the strength of each privacy metric using four intensity indicators: monotonicity, degree of spread, evenness of spread and shared value range. To implement our methodology, we have used open-source Python packages like NumPy [24], SciPy [24], scikit-learn [17], scikit-gof, and mpi4py [7].

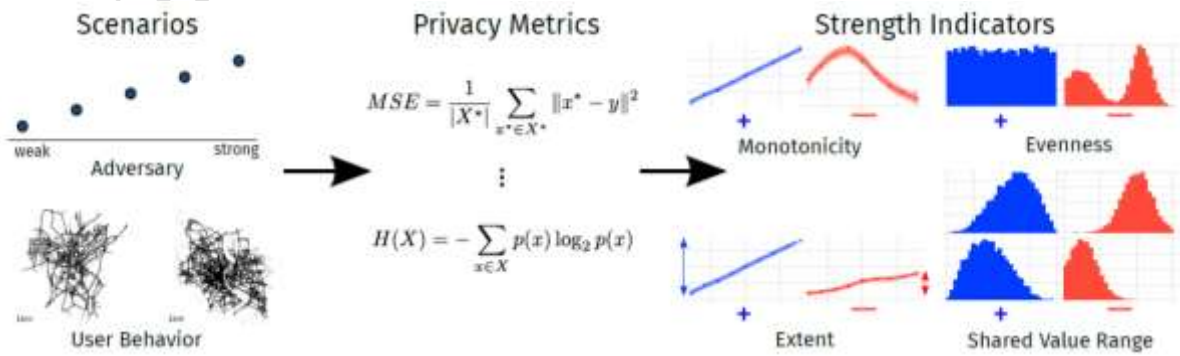

Fig.1. Methodology for determining the effectiveness of data protection metrics. (1) User actions and conduct of adversaries are incorporated into scenarios. (2) The examples are subject to Privacy Metrics. (3) In each case, the

strength of privacy metrics is measured with four reliability indicators: monotonicity, degree of spread, evenness of spread and shared value spectrum.

3.1 Privacy Metrics

We are reviewing 41 privacy metrics suggested in the literature, both in the literature on vehicle networking and in the broader literature on data protection assessment in other application domains.

3.1.1 Uncertainty Metrics

Most metrics depend on the definition of the set of anonymity, i.e., the set of Vehicles which the opponent can not discern. For our estimation the anonymity set consists of all vehicles v to which a non-zero probability is given by the tracker. Most uncertainty metrics use anonymity set entropy variants[20] to measure secrecy, showing how uncertain the opponent is about their estimation p(x).

$$priv_{RE} \equiv H_\alpha(X) = \frac{1}{1-\alpha} log_2 \sum_{x \in X} p(x)^\alpha$$

Normalized Entropy uses max-entropy to standardize its values to [0;1], indicating the degree of uncertainty of the opponent. The maximum value range is likely to make normalized entropy ideal for comparisons between scenarios.

$$priv_{NE} = \frac{H(X)}{H_0(X)}$$

3.1.2 Gaining information / loss measurements

Data gain / loss metrics calculate how much data the attacker receives (or how much privacy the consumer loses) by watching the opponent.

Number of leaked information shows how many vehicles v the opponent can track correctly, i.e., all cases in which the most probable finding corresponds to the correct vehicle. The values depend strongly on the total number of vehicles in a scenario.

$$priv_{ALI} \equiv |V|, \forall v \in V : \max p(x_v) = x_v^*$$

3.1.3 Error Measurements

Expected Distance Error tests the expected Euclidean distance d(x,x*) over multiple time steps t between the true location and the projected location.

$$priv_{EDE} \equiv \frac{1}{|V|T} \sum_{t \in T} \sum_{v \in V} \sum_{x \in X} p(x_{v,t}) d(x, x^*)$$

3.1.4 Performance metrics for the competitor

Performance metrics from adversary measure how likely the adversary is to succeed.

The Privacy Breach Rate shows the adversary's later likelihood of assigning to the true vehicle, provided the findings y from the current phase in time.

$$priv_{PBL} \equiv p(x = x^*|y)$$

3.1.5 Time Metrics

Time to Confusion shows the average time when entropy is below a h-threshold, i.e. the time when the opponent is not confused.

$$priv_{TC} \equiv \ Time\ during\ which\ H(X) < h$$

IV. RESULTS

We rate metrics by intensity for each criteria, and extract detailed metric selection recommendations in Section 5.

4.1 Monotonicity

To explain our findings regarding the need for monotonicity, Fig. 2. In four traffic conditions, shows one metric, the anonymity size set. Every subfigure shows the distribution of metric values for the nine adversary intensity rates using violin plots, and further indicates the confidence intervals (horizontal lines), the region between quartiles (shaded), mean values (bold numbers), and whether higher or lower numbers indicate higher privacy (green line). The supplementary material includes a full collection of violin plots for all metrics and traffic conditions.

Journal of Engineering Sciences

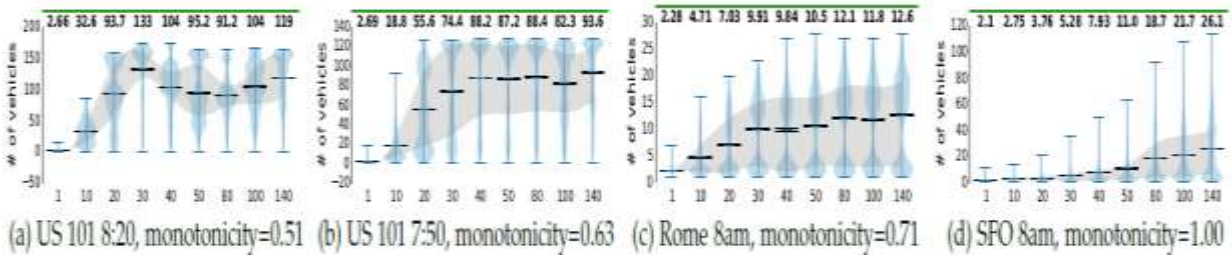

Fig.2. Anonymity size set in four conditions of traffic, ordered from lowest to highest monotonicity

At Fig. 3, We use a heat map to compactly represent the monotonicity ratings. Every square represents one set of results mentioned above in detailed plots of violins. The last square in the third row for instance summarizes Fig. 2a (anonymity set size for US highway 101, 8:20am).

The heat map thus summarizes the results for 15 traffic conditions and 44 metrics, i.e., 660 individual results.

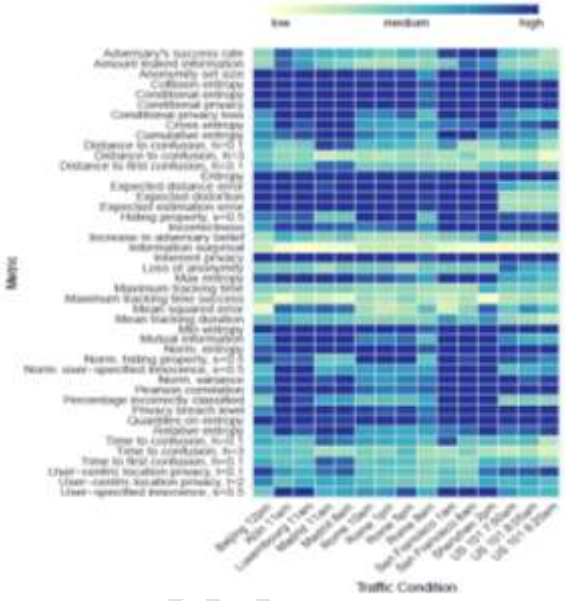

Fig.3. Monotonic Heat map. The colors give the score of monotonicity (from yellow = low to blue = high).

The heat map shows that several metrics have high monotonicity regardless of the traffic condition, for example entropy and the privacy breach level. Very few metrics are nonmonotonic throughout and therefore not recommended, for example information surprisal.

Fig. 4 Provides entropy for the metric with the maximum monotonicity value followed by seven other metrics derived from entropy. We note that several of the metrics that have been proposed to evaluate PETs for vehicular networks, such as the maximum tracking time, the time to confusion, and the mean tracking duration, are not among the strongest metrics (in fact, their average monotonicity scores are below 0.5).

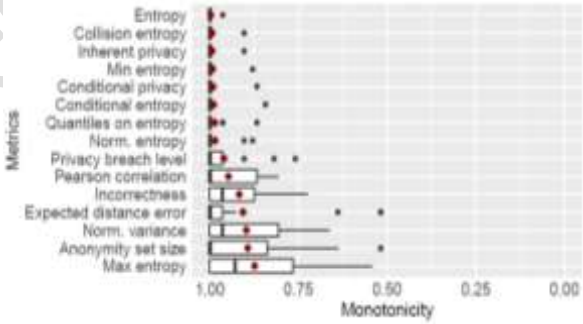

Fig.4. Distribution of monotonicity across all traffic conditions for the strongest 15 metrics.

4.2. Extent and Evenness of Spread

In some traffic conditions, even the metrics with the highest ranges and evenness scores may be low. Hence, their suitability for in-scenario comparisons can be condition-specific and should be checked before using the metrics.

Journal of Engineering Sciences
Vol 11, Issue 4 ,April/2020
ISSN NO:0377-9254

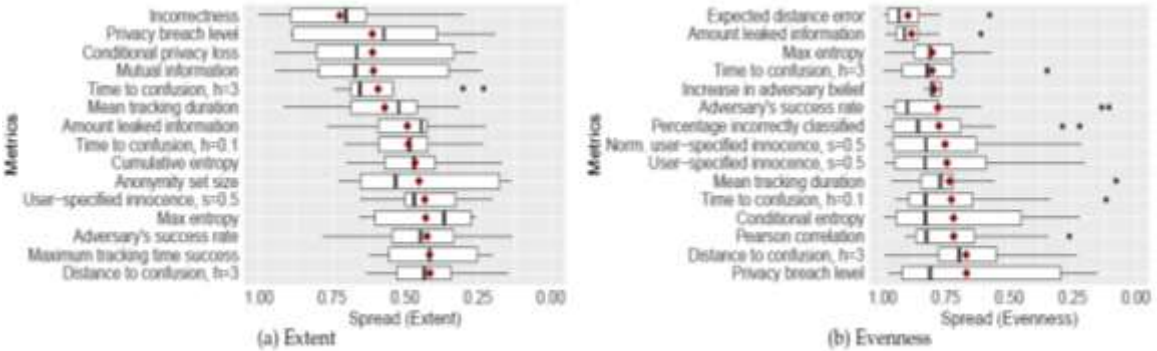

Fig.5. Distribution of the metric's distributed across all traffic conditions for the maximum 15 metres.

Metrics with a high level of monotonicity do not necessarily score highly in spread. The metric with the highest monotonicity score, for example, entropy, has only medium extent and evenness scores (Fig. 5).

4.3. Shared Value Range

Metrics that use the same range of values regardless of traffic situation are more suitable for comparing the degree of privacy between the scenarios. Fig. 6. Lists the 15 measures with the highest score on a common range of values. We note that certain metrics with a high shared value spectrum score very low on monotonicity, e.g. increases in adversary confidence and unexpected knowledge.

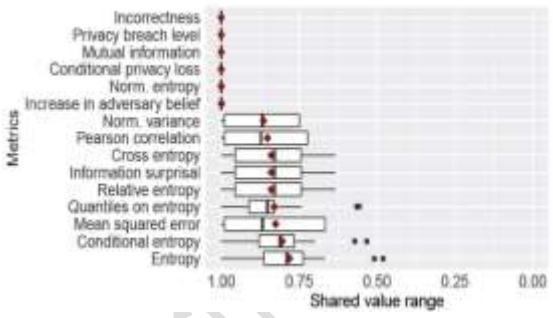

Fig.6. Distribution of the shared value spectrum across all traffic conditions for the best 15 metres.

V. DISCUSSION

We addressed 41 privacy metrics and rated them according to four criteria: monotonicity, duration, evenness, and set of shared values.

5.1 Weak Metrics

We note that some of the metrics specifically proposed for use in vehicle networks score low on monotonicity and are in the lower half of our overall metric ranking. These metrics include the mean duration of tracking, the time / distance to confusion and the maximum time to track. Hence we recommend replacing these metrics with other metrics stronger in vehicle network scenarios.

5.2 PET Technology Aid Visualisation

Our visualization of privacy metrics on city maps showed that privacy often depends on the road layout and traffic density in a city. A possible consequence for the design of PETs is that it may make sense to apply one PET in city centers with dense traffic, and choose another PET for outskirts with less dense traffic, or to adjust parameter settings to provide adequate privacy in all areas.

5.3 Metrics Suites

Even the best metrics in our experiments do not perform well in all traffic conditions, as shown in our box plots and heat maps. One solution to this problem is to test all metrics before applying them to new traffic conditions. Therefore, a better solution is to integrate many metrics into a metrics package, i.e. to work with several metrics at all times. When choosing a metrics suite, we recommend considering three aspects: only use metrics with a high monotonicity score , include metrics from different categories, e.g., uncertainty, information gain/loss and error, include metrics which are particularly strong for comparisons within the scenario as well as metrics which are strong for comparisons between scenarios.

VI. CONCLUSION

We have introduced four novel criteria for assessing the strength of data protection metrics: monotonicity, extent, evenness, and range of shared values. These criteria measure the consistency of metrics of privacy and their suitability for comparisons of privacy levels within scenario and inter scenario. Our key findings are that (1) some current metrics have low monotonicity ratings, i.e. they that misjudge the intensity of new privacy-

enhancing technologies (PETs), (2) no single metric dominates all requirements and traffic conditions, and (3) visualization may illustrate where privacy depends on road layout and can thus help PET design. Based on these results, we suggest that metrics suites always be used when testing new PETs.

REFERENCES

[1] D. Alexander & J. Smith, "Security Technology in Public: Confounding Face Recognition," in the 3rd International Workshop on Technologies Enhancing Privacy (PET). Dresden, Germany: LNCS springer, vol. 2760, Mar. 2003, pp. 88–106.

[2] H. Blackman, R. Popoli, Modern Tracking Systems design, and analysis. Boston: Publishers at Artech House, Jun. 1999.

[3] D. Eckhoff, C. Sommer, "Conducting big data? Vehicular Networking Privacy Concerns, "IEEE Security & Privacy vol. 12, no, pp. 77–79, January 2014.

[4] In Z. Kargl, Ma, F., and M. Weber, "Measuring Long Term Location Privacy in Vehicle Communication Systems," Communications Devices, vol. 33, 12, pp. 1414–1427, 2010 Jul.

[5] I. Wagner, D. Eckhoff, "Vehicle Networks Use Simulation Privacy Evaluation," in Winter Simulation Conference (WSC), Savannah, GA, United States, Dec. 2014, pp. 3155–3166.

[6] A. Wasef, X. Shen, "REP: VANET Location Protection Using Random Encryption Periods," Mobile Networks and Applications, vol. No. 1 of 15, pp. 172–185, Feb. 2010.

[7]B. Wiedersheim, F. Kargl, Z. Ma and P. Papadimitratos, "Security in Inter-vehicular Networks: Why Simple Pseudonym Switch Is Not Enough," at the 7th International Wireless On-Demand Network Systems and Services Conference (WONS), Kranjska Gora, Slovenia, Feb. 2010, pp. 176–183.

Journal of Engineering Sciences