National Congress

“Open Science – The Way Forward”

Trust-based traffic assessment model for congestion control in vehicular networks

Rihab ABIDI

Supervisory team: Nadia BEN AZZOUNA
Ghaleb HOBLOS
Wassim TROJET
Nabil SAHLI

Organization de la thèse

- Thesis jointly supervised by the **University of Tunis** and **Normandy University**

- Doctoral schools: **Sciences of management** and **Mathematics, Information, Systems Engineering**

Mathématiques, Information, Ingénierie des Systèmes

- Research units: SMART Lab et IRSEEM

Outline

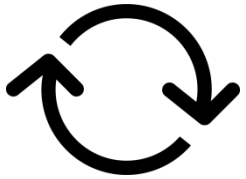
- Introduction
- Realized work
- Work in progress
- Future works

Context

" Traffic congestion condition on road networks occurs as a result of excessive use of road infrastructure beyond capacity, and slower speeds, longer trip hours and increased vehicular queuing characterize it." (Agyapong, F., & Ojo, T. K. ,2018).

Recurring causes :

- Infrastructure
- Rush hours



Non-recurring causes :

- Environment
- Mecanical
- Human

Impacts:

- Safety and health: 1.35 million people / year die from traffic incidents around the world (WHO, 2020).
- The environment: 3 billion tonnes of CO2 emitted into the atmosphere in the European Union (IEA, 2014).
- The economy: The total cost of lost productivity was $ 87 billion (Sean Fleming, 2019).

Problematic

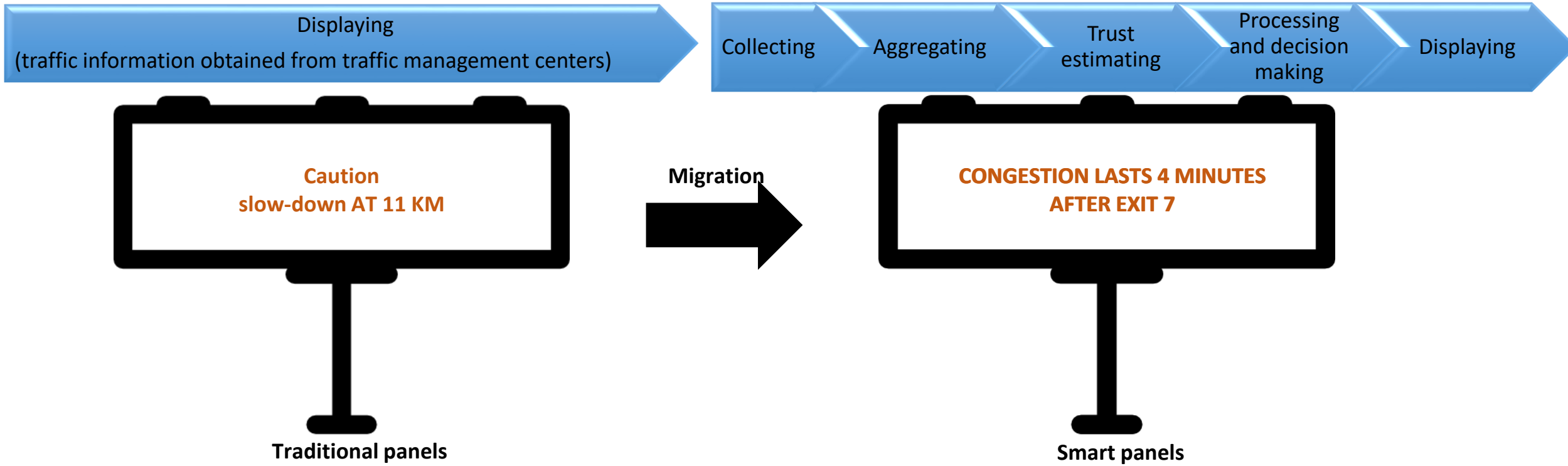
Solution:
A system that estimates current traffic state and warns drivers of possible traffic congestions or accidents.

Constraints:
- Nodes are exposed to different security threats
- The accuracy of the traffic estimation is affected by the quality of the exploited data
- The decision-making process must be carried out in real time

Implementation of a **trust** management system

- How to assess the accuracy and relevance of the sensed traffic data?
- How to design a trust management model that is more comprehensive and adapted to the constraints of ITSs?

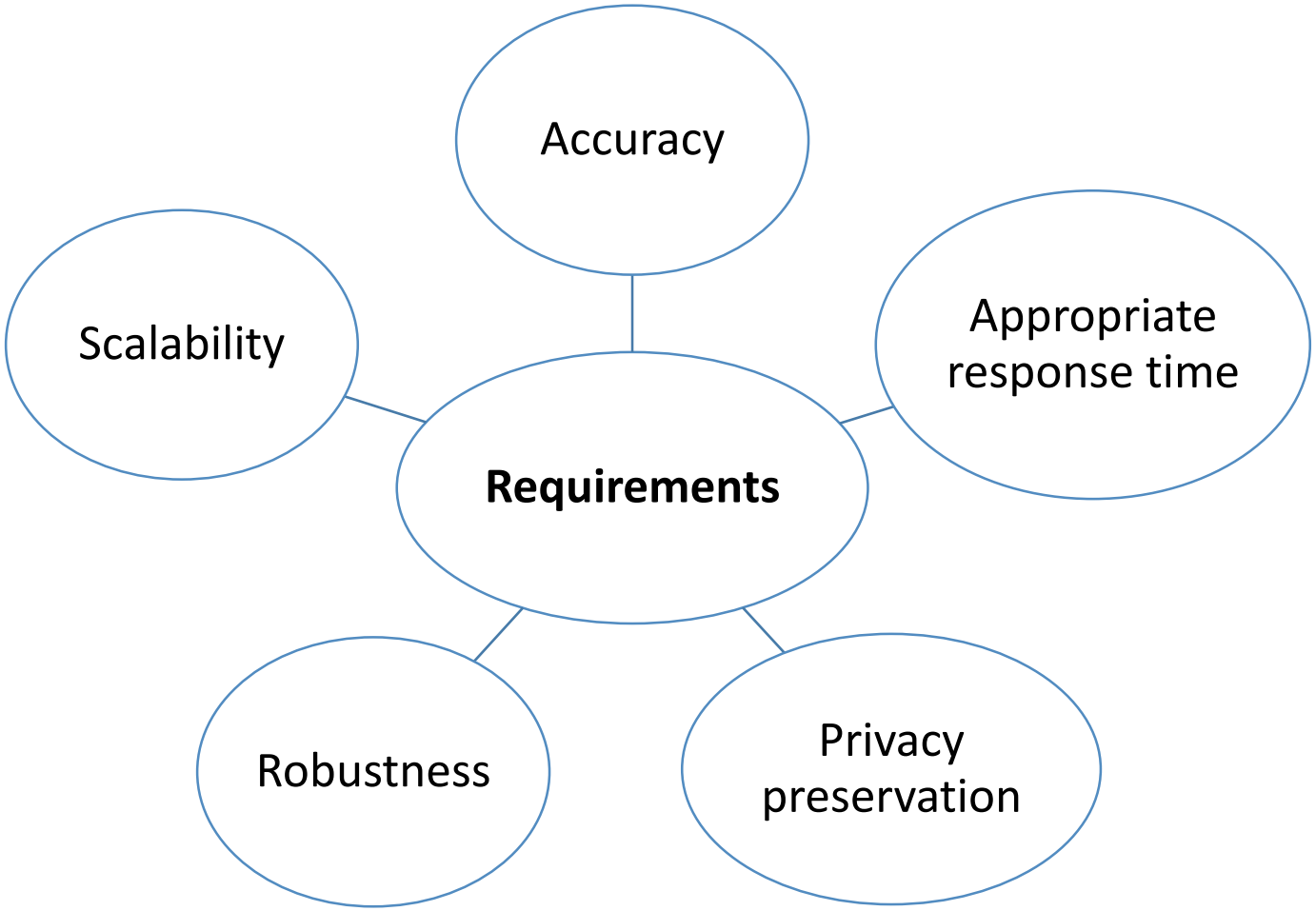
Vision

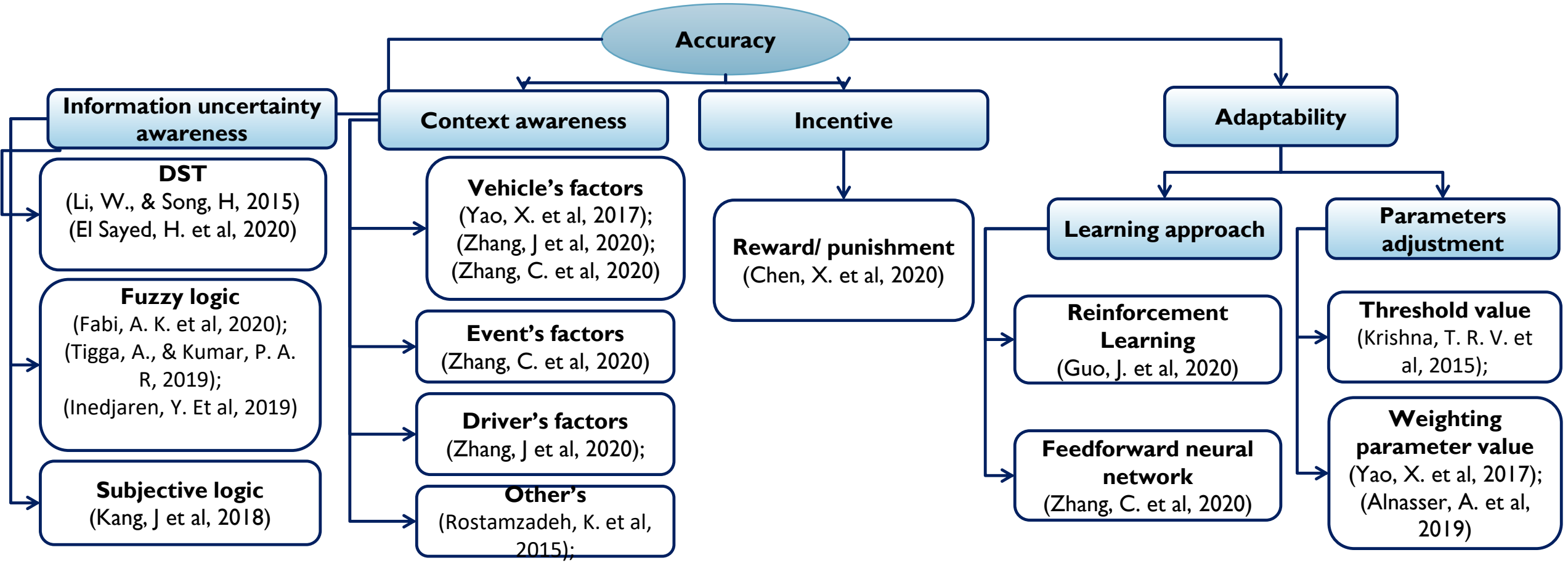

Displaying
(traffic information obtained from traffic management centers)
Collecting
Aggregating
Trust estimating
Processing and decision making
Displaying
Caution
slow-down AT 11 KM
Migration
CONGESTION LASTS 4 MINUTES
AFTER EXIT 7
Traditional panels
Smart panels

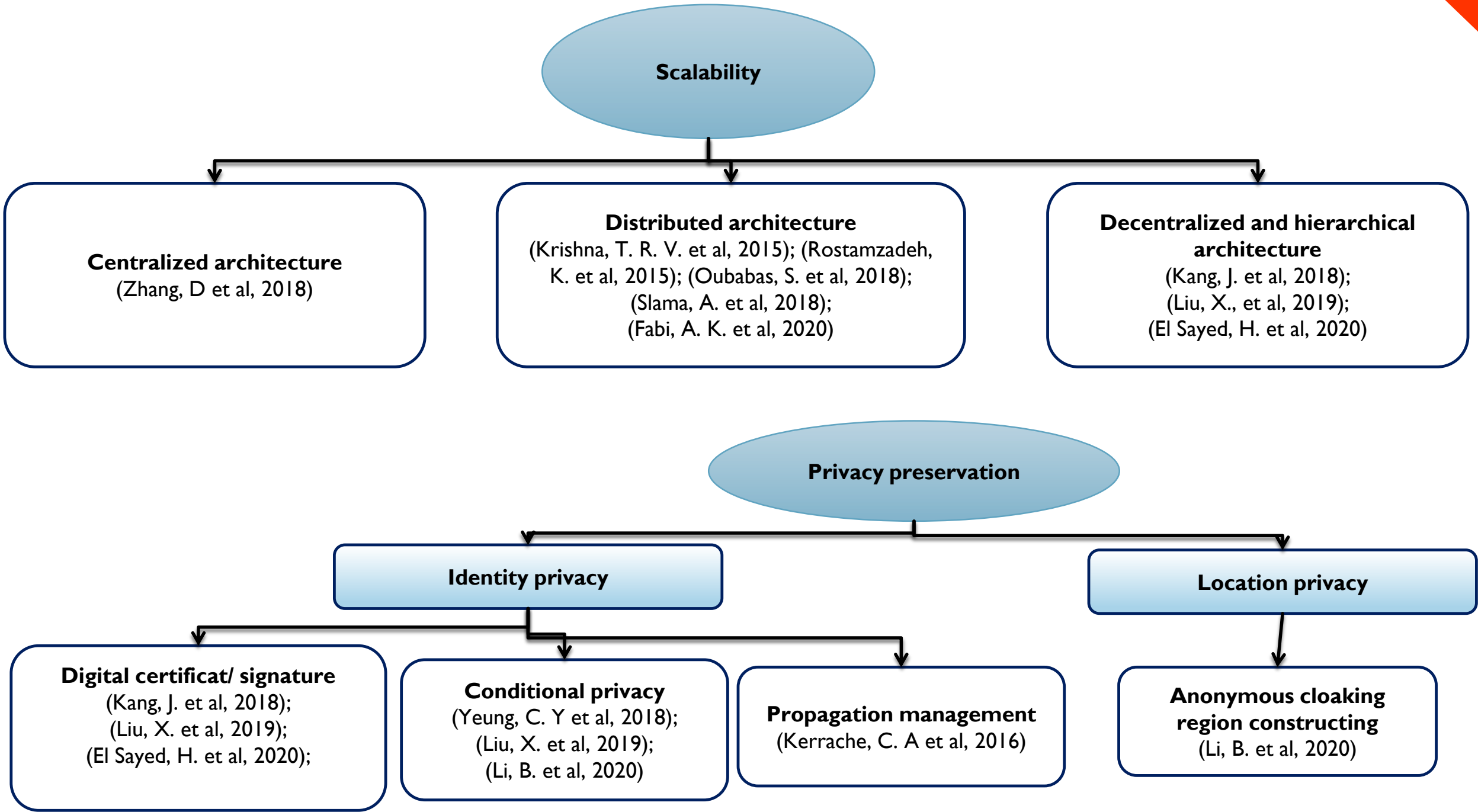
Dynamic Message Sign (DMS)

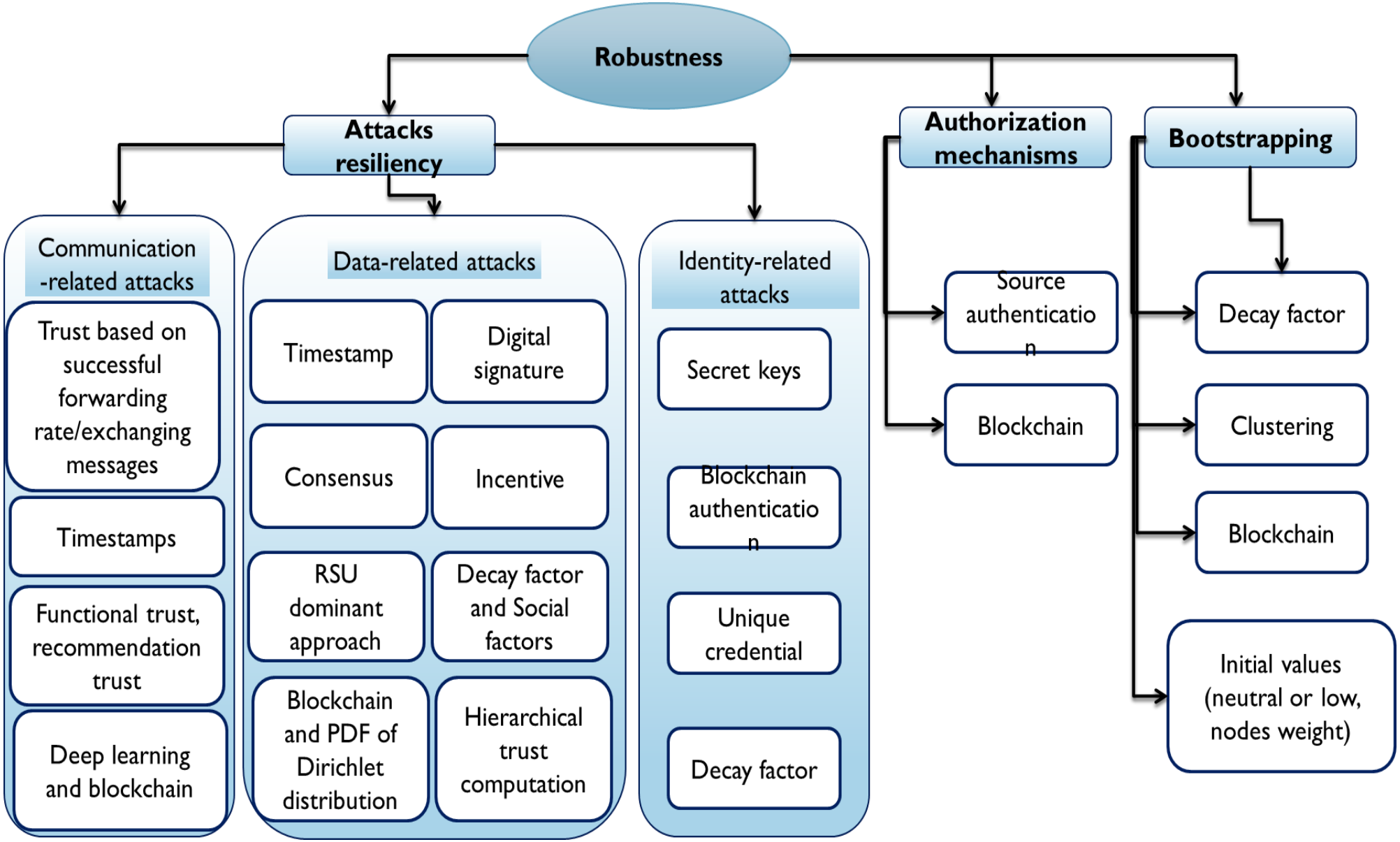
State of the art

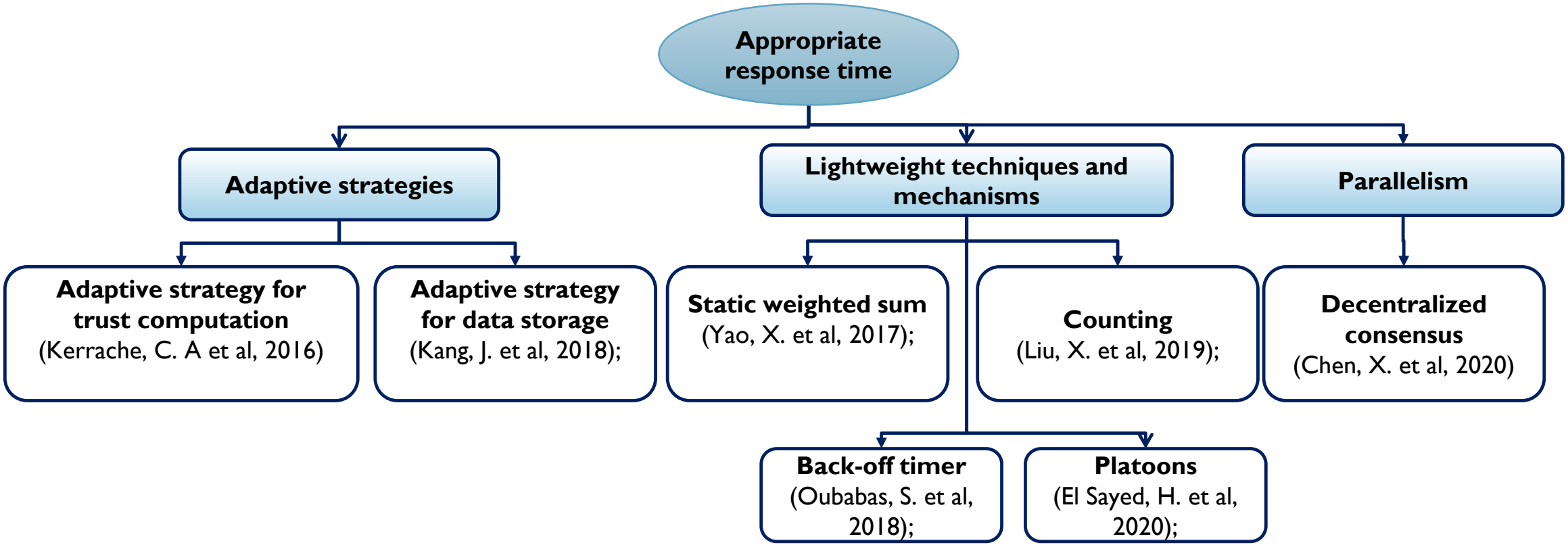
Scope: Identifying the requirements considered in the proposed trust models and detecting the mechanisms used to fulfil them.




Accuracy
Information uncertainty awareness
DST
(Li, W., & Song, H, 2015)
(El Sayed, H. et al, 2020)
Fuzzy logic
(Fabi, A. K. et al, 2020);
(Tigga, A., & Kumar, P. A. R, 2019);
(Inedjaren, Y. Et al, 2019)
Subjective logic
(Kang, J et al, 2018)
Context awareness
Vehicle's factors
(Yao, X. et al, 2017);
(Zhang, J et al, 2020);
(Zhang, C. et al, 2020)
Event's factors
(Zhang, C. et al, 2020)
Driver's factors
(Zhang, J et al, 2020);
Other's
(Rostamzadeh, K. et al, 2015);
Incentive
Reward/ punishment
(Chen, X. et al, 2020)
Adaptability
Learning approach
Reinforcement Learning
(Guo, J. et al, 2020)
Feedforward neural network
(Zhang, C. et al, 2020)
Parameters adjustment
Threshold value
(Krishna, T. R. V. et al, 2015);
Weighting parameter value
(Yao, X. et al, 2017);
(Alnasser, A. et al, 2019)


Scalability
Centralized architecture
(Zhang, D et al, 2018)
Distributed architecture
(Krishna, T. R. V. et al, 2015); (Rostamzadeh, K. et al, 2015); (Oubabas, S. et al, 2018); (Slama, A. et al, 2018); (Fabi, A. K. et al, 2020)
Decentralized and hierarchical architecture
(Kang, J. et al, 2018); (Liu, X., et al, 2019); (El Sayed, H. et al, 2020)
Privacy preservation
Identity privacy
Location privacy
Digital certificat/ signature
(Kang, J. et al, 2018); (Liu, X. et al, 2019); (El Sayed, H. et al, 2020);
Conditional privacy
(Yeung, C. Y et al, 2018); (Liu, X. et al, 2019); (Li, B. et al, 2020)
Propagation management
(Kerrache, C. A et al, 2016)
Anonymous cloaking region constructing
(Li, B. et al, 2020)


Robustness
Attacks resiliency
Authorization mechanisms
Bootstrapping
Communication -related attacks
Trust based on successful forwarding rate/exchanging messages
Timestamps
Functional trust, recommendation trust
Deep learning and blockchain
Data-related attacks
Timestamp
Digital signature
Consensus
Incentive
RSU dominant approach
Decay factor and Social factors
Blockchain and PDF of Dirichlet distribution
Hierarchical trust computation
Identity-related attacks
Secret keys
Blockchain authenticatio n
Unique credential
Decay factor
Source authenticatio n
Blockchain
Decay factor
Clustering
Blockchain
Initial values (neutral or low, nodes weight)


Appropriate response time
Adaptive strategies
Lightweight techniques and mechanisms
Parallelism
Adaptive strategy for trust computation
(Kerrache, C. A et al, 2016)
Adaptive strategy for data storage
(Kang, J. et al, 2018);
Static weighted sum
(Yao, X. et al, 2017);
Counting
(Liu, X. et al, 2019);
Decentralized consensus
(Chen, X. et al, 2020)
Back-off timer
(Oubabas, S. et al, 2018);
Platoons
(El Sayed, H. et al, 2020);

Trust management model

Objective:

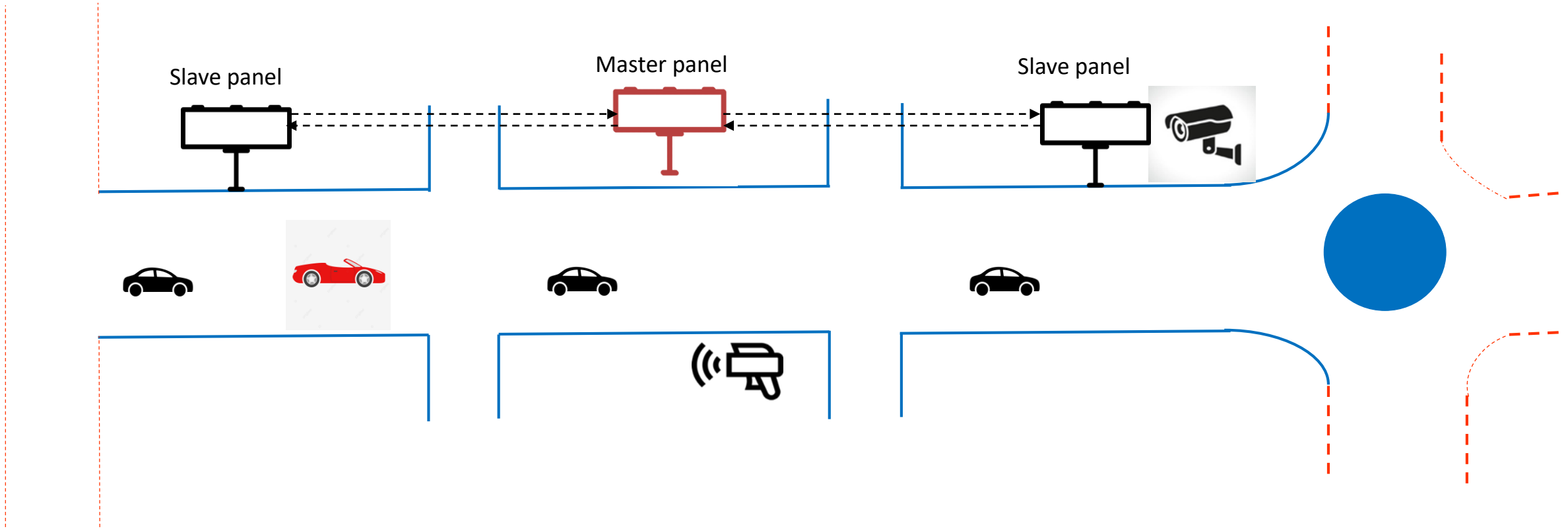
Develop a hybrid trust model to:

- Evaluate the trustworthiness of traffic events
- Evaluate the trustworthiness of information sources

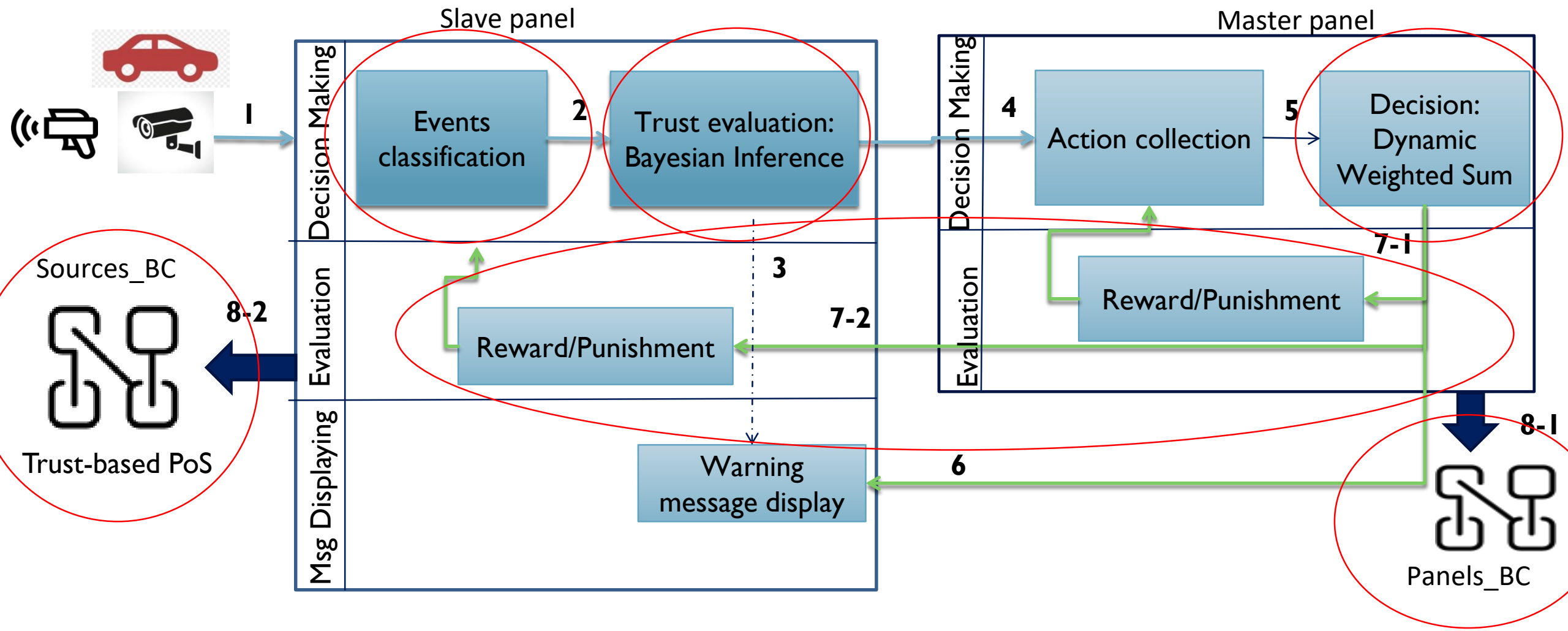
Requirements:

- Accuracy
- Robustness
- Scalability
- Privacy preservation
- Short response time

Vehicular network



Panel architecture

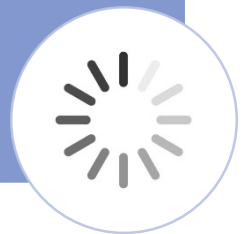


- Study of the state of the art
- Submission of a survey paper

Realized work

- Development of a new trust management model
- Execution of test scenarios for model validation
- Writing a journal article

Work in progress



- Assessing the Trust Value of Master Panels
- Development of a dynamic panel clustering model
- Consideration of more generic granularities

Future works

Thank you for your attention

References

- Agyapong, F., & Ojo, T. K. (2018). Managing traffic congestion in the Accra central market, Ghana. Journal of Urban Management, 7(2), 85-96.
- WHO. Road traffic injuries. https://www.who.int/news-room/fact-sheets/detail/road-traffic-injuries. (21 June 2021), accessed December 18, 2021.
- Sean Fleming. Traffic congestion cost the US economy nearly $87 billion in 2018. https://www.weforum.org/agenda/2019/03/traffic-congestion-cost-the-us-economy-nearly-87-billion-in-2018. (07 Mar 2019), accessed December 18, 2021.
- Zhang, D., Yu, F. R., Yang, R., & Tang, H. (2018, October). A deep reinforcement learning-based trust management scheme for software-defined vehicular networks. In Proceedings of the 8th ACM Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications (pp. 1-7).
- Krishna, T. R. V., Barnwal, R. P., & Ghosh, S. K. (2015). CAT: Consensus-assisted trust estimation of MDS-equipped collaborators in vehicular ad-hoc network. Vehicular Communications, 2(3), 150-157.
- Rostamzadeh, K., Nicanfar, H., Torabi, N., Gopalakrishnan, S., & Leung, V. C. (2015). A context-aware trust-based information dissemination framework for vehicular networks. IEEE Internet of Things journal, 2(2), 121-132.

- Oubabas, S., Aoudjit, R., Rodrigues, J. J., & Talbi, S. (2018). Secure and stable vehicular ad hoc network clustering algorithm based on hybrid mobility similarities and trust management scheme. Vehicular Communications, 13, 128-138.
- Slama, A., Lengliz, I., & Belghith, A. (2018, November). TCSR: an AIMD Trust-based Protocol for Secure Routing in VANET. In 2018 International Conference on Smart Communications and Networking (SmartNets) (pp. 1-8). IEEE.
- Fabi, A. K., & Thampi, S. M. (2020). A psychology-inspired trust model for emergency message transmission on the Internet of Vehicles (IoV). International Journal of Computers and Applications, 1-11.
- El Sayed, H., Zeadally, S., & Puthal, D. (2020). Design and evaluation of a novel hierarchical trust assessment approach for vehicular networks. Vehicular Communications, 24, 100227.
- Zhang, J., Zheng, K., Zhang, D., & Yan, B. (2020). AATMS: An anti-attack trust management scheme in vanet. IEEE Access, 8, 21077-21090,
- Zhang, C., Li, W., Luo, Y., & Hu, Y. (2020). AIT: An AI-Enabled Trust Management System for Vehicular Networks Using Blockchain Technology. IEEE Internet of Things Journal, 8(5), 3157-3169.

- Chen, X., Ding, J., & Lu, Z. (2020). A decentralized trust management system for intelligent transportation environments. IEEE Transactions on Intelligent Transportation Systems.
- Alnasser, A., Sun, H., & Jiang, J. (2019). Recommendation-based trust model for vehicle-to-everything (V2X). IEEE Internet of Things Journal, 7(1), 440-450.
- Guo, J., Li, X., Liu, Z., Ma, J., Yang, C., Zhang, J., & Wu, D. (2020). TROVE: A context-awareness trust model for VANETs using reinforcement learning. IEEE Internet of Things Journal, 7(7), 6647-6662.
- Li, B., Liang, R., Zhu, D., Chen, W., & Lin, Q. (2020). Blockchain-based trust management model for location privacy preserving in VANET. IEEE Transactions on Intelligent Transportation Systems, 22(6), 3765-3775.
- Liu, X., Huang, H., Xiao, F., & Ma, Z. (2019). A blockchain-based trust management with conditional privacy-preserving announcement scheme for VANETs. IEEE Internet of Things Journal, 7(5), 4101-4112.
- Kerrache, C. A., Calafate, C. T., Cano, J. C., Lagraa, N., & Manzoni, P. (2016). Trust management for vehicular networks: An adversary-oriented overview. IEEE Access, 4, 9293-9307.
- Kang, J., Yu, R., Huang, X., Wu, M., Maharjan, S., Xie, S., & Zhang, Y. (2018). Blockchain for secure and efficient data sharing in vehicular edge computing and networks. IEEE Internet of Things Journal, 6(3), 4660-4670.