BOOTSTRAPPING TRUST IN NDN-BASED VEHICULAR NETWORKS USING SWIFT TRUST

Sanjeev Kaushik Ramani[*], *Manushri Viswanath*[^], *Jelena Jones*[#], *Alex Afanasyev*[*]

[*] *Florida International University,* [^] *Rensselaer Polytechnic Institute,* [#] *Clafflin University*

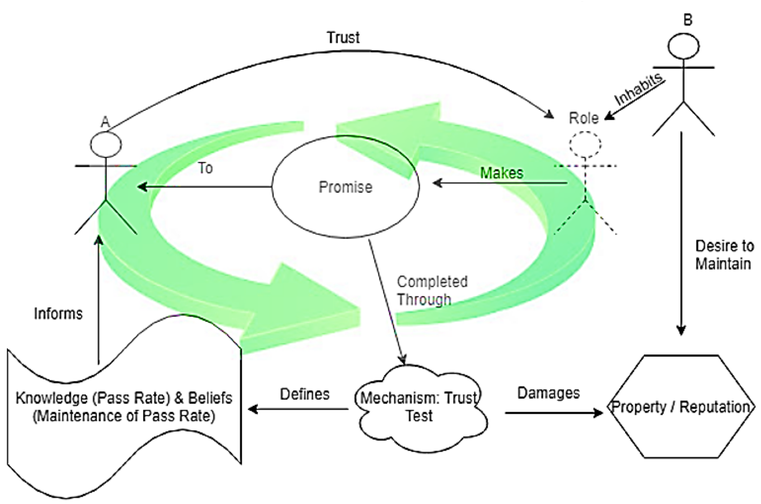
ABSTRACT

In a vehicular communication scenario, there is a necessity for establishing temporary trust amongst communicating vehicles to accomplish certain tasks. The proposed Named Data Networking (NDN) architecture enables seamless communication in vehicular networking scenarios by focusing on application-named data retrieval and providing security features at the networking level. This project explores how Swift Trust model can be applied in a vehicular environment with NDN-based communication. As an initial step in this exploration, we design a task-oriented method of establishing trust based on request-response communication.

SWIFT TRUST

Swift trust is a form of trust occurring in temporary organizational structures, which can include quick starting groups or teams. It was first explored by Debra Meyerson and colleagues in 1996. In swift trust theory, a group or team assumes trust initially, and later verifies and adjusts trust beliefs accordingly. It is well suited for a dynamic environment like Internet of Things (IoV), Vanets etc.

The figure below shows the general structure for Swift Trust and the various parties involved and their role in Trust establishment. In this poster, we try to showcase how SWIFT Trust could be used to bootstrap trust in Vanets.

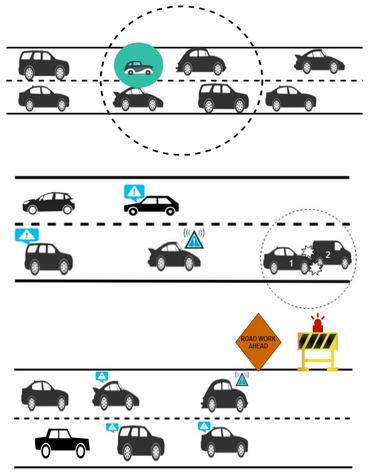


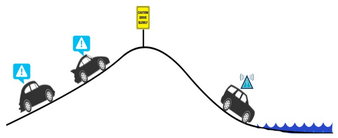
ASSUMPTIONS

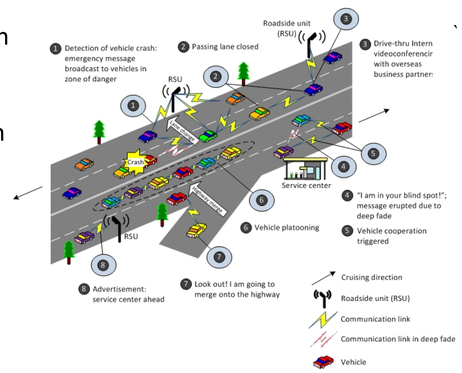
- Sensors have enough storage to perform proposed applications
- Vehicles have the computational capability to process and reply to the heartbeat and al-carte messages sent as a part of request

TARGETED APPLICATION DOMAIN: VANETS

- Notification for lane changes
  - Continuous process
- Crash Detection and reporting:
  - location of the accident
  - time the accident occurred
  - number of vehicles involved
- Road-work notifications
  - location of the affected area
  - speed of vehicles ahead
- Vehicle Platooning
  - speed of vehicles in path
- Commercial delivery
  - path to delivery location







MESSAGE TYPES

Heartbeat msg → /<vehicle-name>/SWIFT/<granularity>/HeartBeat/<msg-id>

/Tim_Corolla/SWIFT/NorthWest/HeartBeat/msg-10

A la carte msg → /<vehicle-name>/SWIFT/<granularity>/alacarte/<msg-id>

/San_Honda/SWIFT/SouthEast/Playlist_English/

/Raj_BMW/SWIFT/North/AudioBooks_Spanish/

Emergency → /<vehicle-name>/SWIFT/<granularity>/ALERT/<msg-id>

/FIU_Security/SWIFT/WEST_Wing_PG6/Crash_Report/msg-1

Other Message types:

Probe Vehicle Data message →

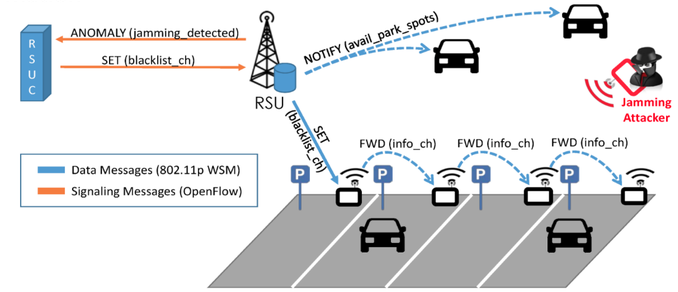
/<vehicle-name>/SWIFT/<granularity>/PROBE/<msg-id>

Common safety request message →

/<vehicle-name>/SWIFT/<granularity>/SAFETY/<msg-id>

TRUST METRICS

- Each vehicle assumes the role of a possible trusted entity with the desire to maintain a good reputation among other vehicles. While occupying this role, they make a promise to the requesting entity to accomplish a task at hand without a malicious intent.
- Trust computation is based on a weighted sum of questions asked in the various above mentioned messages and the comparison of the results obtained from the neighbors. Weights could be:
  - **Social** (30% weight) - related to things outside of the vehicle
  - **Task-Oriented** (70% weight) - related to sensors and logical information



FUTURE WORK

- Implementation and simulation of the proposed scenarios
- Integration of other trust frameworks in combination with Swift Trust to create a unique robust trust mechanism for NDN applications
- Security analysis and evaluation

REFERENCES

1. Yan, Z., Zhang, P., & Vasilakos, A. V. (2014). A survey on trust management for Internet of Things. Journal of Network and Computer Applications, 42, 120-164. doi:10.1016/j.jnca.2014.01.014
2. Harwood, W. T. (2012). The Logic of Trust. York: Publisher not identified.
3. Murthy, D., Rodriguez, A., & Lewis, J. (2013). Examining the Formation of Swift Trust within a Scientific Global Virtual Team. 2013 46th Hawaii International Conference on System Sciences. doi:10.1109/hicss.2013.211
4. C. A. Kerrache, C. T. Calafate, J. Cano, N. Lagraa and P. Manzoni, "Trust Management for Vehicular Networks: An Adversary-Oriented Overview," in IEEE Access, vol. 4, pp. 9293-9307, 2016.

ACKNOWLEDGEMENTS

This work is partially supported by the National Science Foundation for providing the Grant: CNS-1560134 and the US Army Grant Number W911NF-12-R-0012 for funding the project.