Section 3: Week 6: IoT and Assisted Driving

Nate Bachmeier

TIM-7010: Computer Networking and Mobile Computing

August 4, 2019

North Central University

# Table of Contents

[IoT and Assisted Driving 2](#_Toc15855695)

[Literature Review 2](#_Toc15855696)

[An Internet of Cars (2012). 2](#_Toc15855697)

[Smart Cities: an IoT-centric Approach (2014) 3](#_Toc15855698)

[NDN IoT Content Distribution Model 3](#_Toc15855699)

[Hardware and Embedded Security in the Context of Internet of Things (2013) 4](#_Toc15855700)

[Lightweight Secure-Boot Architecture for RISC-V System-on-Chip (2019) 5](#_Toc15855701)

[Secure and Efficient Management (2015) 6](#_Toc15855702)

[Conclusions 6](#_Toc15855703)

[References 8](#_Toc15855704)

# IoT and Assisted Driving

“Vehicular collisions, which kill thirty thousand people in the US annually and injure almost a million more, maybe tackled by using embedded wireless sensors, monitors, and actuators in automobiles (Kanuparhi, Karri, & Addepalli, 2013).” Due to several open problems, society has not realized that vision. If we can successfully deploy IoT sensor networks and create smart roads, the potential gains to safety are enormous.

# Literature Review

## An Internet of Cars (2012).

If vehicles are going to share sensor data, then a notion of identity needs to exist for each participant (Speed & Shingleton, 2012). Without an identification service, it would not be possible to determine metrics are coming from ‘this or that’ car. Speed and Shingleton propose a system that relies on the car’s registration information, similar to a barcode. They describe an integration into smart cities that tracks the drivers and assesses common route patterns.

There are advantages to this approach; however, they do not address the drivers need for privacy. Perhaps there are multiple classes of drivers such as public buses, rideshare vehicles, and private commuters. Each of these classes requires a different level of privacy before they are willing to participate in that vision.

One solution could be to allow each vehicle to control the lifespan of their registration identifier. For instance, the public bus might be willing to base its identity on the VIN while the private commuter rotates with the engine.

This level of anonymity would protect the driver’s personal information and still enable smart roads to efficiently operate. Analogously, today we see the vehicle next to us is a Honda Prius—we do not know the driver is named John Snow.

## Smart Cities: an IoT-centric Approach (2014)

After solving identity, the next layer to address is the organization and publication of these open datasets. Smart cars will need to consume data feeds from traffic lights, road sensors, accident reports, and construction schedules, to name a few. One solution is to decompose smart cities into smart city *hubs*, where a hub is a logical unit such as a shopping district or residential neighborhood (Lea & Blackstock, 2014).

Lea and Blackstock examined the implementation of two smart cities, one in the United Kingdom the other in Canada. With both locations, an efficient data catalog was critical to the project’s success. They attributed this to reducing the learning curve, resulting in more developers creating more applications available.

Over the last five years, several American cities, such as Seattle and New York, have created open data platforms. The easy access to data has enabled dozens of high-quality applications; however, they are specific to that location.

Small development studios are willing to build dedicated apps for a given city, but more prominent corporations are unwilling to enter the space. Their userbase spans the entire country and needs it to be usable on a national level. If they must implement a data adaptor of every metropolitan area, the development cost will be too great to justify. Until businesses, city planners, and hardware manufacturers agree on open standards; there will be challenges sharing the data and making it fully discoverable.

## NDN IoT Content Distribution Model

After standardizing the data schemes, they might become discoverable through Name Data Networks (NDN). Under NDN, publishers create signed content under different namespaces, and then consumers can discover and fetch those resources (Shilton, Burke, Caffy, & Zhang, 2016). Software-Defined Networking (SDN) can cache these resources directly in the networking layer and expose them through forwarding rules.

A smart vehicle might know that it is driving down Jackson toward 7th Avenue, and use this information to request content for /USA/Washington/Seattle/Jackson/7th avenue. Through a separation of duties, the network could then return an array of data catalog entries relevant to that corner. If data is not available for the child directory, then the protocol can fall back to the parent directory. Such a scheme addresses discoverability concerns and provides extensibility for future requirements.

Having a simple system for anonymous content to be discoverable, published, and consumed enables several core scenarios. Though it also introduces complexities with data authenticity. What prevents a malicious user from reporting that a road is under construction and causing all cars to divert to other routes? Accomplishing this feat could reduce their travel time at the expense of the broader community.

## Hardware and Embedded Security in the Context of Internet of Things (2013)

Data integrity, identity management, trust management, and privacy are four areas of security that impact all IoT scenarios (Kanuparhi, Karri, & Addepalli, 2013). Kanuparhi et al. continue to provide examples across vehicular, elderly homes, and smart city verticles. They propose Physical Unclonable Functions (PUF) as potential mitigations.

Given the heterogeneous nature of the Internet of Things ecosystems, it might be unrealistic to assume the additional hardware is available. Commodity server software addresses these limitations by using Public Key Infrastructures (PKI).

PKI topologies allow chains of trust to authenticate the authenticity of data. For instance, a traffic light could publish data signed with its device certificate. The smart city hub signs the device certificate with its certificate. These cross signatures recurse outward to state or national authorities. If a security-critical event occurs, then the, e.g., traffic light’s signing identity can be revoked and its published data invalidated.

There are naturally complexities to operating a PKI that could contain records for every vehicle and device on the road, though it a solvable problem (Cincilla, Hicham, & Charles, 2016). Evaluations with simulation networks conclude that modern technologies could handle these massive workloads, provided inevitable trade-offs occur. For instance, the system administrators would need to balance costs with acceptable latencies.

## Lightweight Secure-Boot Architecture for RISC-V System-on-Chip (2019)

When devices transition from hardware-based security solutions toward software implementations, there are additional attack vectors. For example, an attacker can physically modify the traffic light’s disk image. Secure boot protections can detect these scenarios and abort the initialization of the device (Jawad, Ming, Vikramkumar, Shivan, & Anupam, 2019).

Jawad et al. provide a hardware-based implementation for System-on-Chip (SoC) systems to ensure every stage in the boot process is signed. Like previous designs, they rely on the Trusted Platform Module (TPM) as a mechanism to validate each signature. If code authentication fails, then the solution aborts the initialization.

Given the ubiquitous availability of high-speed wireless, these sensors could stream their operating system image during secure boot. Then it would not be possible for many physical attacks to compromise integrity, though there can be challenges scaling such a solution globally.

Consider the scenario where a storm disrupts wireless signal or rural areas; it might be unacceptable for entire sensor networks to be offline. If smart vehicles need to download their image from Ford or Tesla, then what happens when those sites cannot be reached? Most likely they would use a locally cached copy. The local cache introduces a new attack surface that would require signatures authenticated during secure boot.

## Secure and Efficient Management (2015)

A mechanism needs to exist to propagate policy and deploy security patches to both smart vehicles and the broader sensor networks within the road (Kim, 2015). Kim proposes a Policy Gateway, with multi-casting capabilities as a possible solution. Details into his solution are limited but seem to focus on multi-party encryption schemes.

The policy distribution appears to be another area where NDN can assist. When the car starts, it could query the example namespace /Suburu/Forester/2018/ and discover the manufacture recommended policy. Suburu can sign that policy, guaranteeing its authenticity after download.

The verified policy could request the vehicle download updated system images through Content Delivery Networks (CDN). Existing CDN technologies can efficiently distribute files to millions of consumers. These capabilities remove the need to devise a new multi-casting strategy.

# Conclusions

Vehicular accidents inflict injuries to over a million people per year and requires technologies, such as IoT devices, to reduce the instances. Despite interest from the community, these solutions are available in limited capacities. Before wider adoption occurs, several key challenges need resolutions.

Mechanisms for identifying vehicles and devices on the roadway need while respecting the driver’s privacy are needed. Then systems for collecting and distributing data catalogs through open standards must be defined.

If the data feeds are not discoverable and verifiable, then drivers cannot trust them. Supporting end-to-end verification is more complicated than merely provisioning a few certificates. It expands into the need for secure boot architectures and policy management.

While none of these challenges are impossible, each step along the way needs agreement from businesses, hardware vendors, and city planners. Getting buy-in from each stakeholder is a difficult task, yet if accomplished would improve the quality of life for over a million people per year. If that’s not a problem worth solving, I’m not sure what is.

# References

Cincilla, P., Hicham, O., & Charles, B. (2016). Vehicular PKI Scalability-Consistency Trade-Offs in Large Scale Distributed Scenarios. *2016 IEEE Vehicular Networking Conference (VNC)*.

Jawad, H., Ming, W., Vikramkumar, P., Shivan, B., & Anupam, C. (2019). Lightweight Secure-Boot Architecture for RISC-V System-on-Chip. *20th International Symposium on Quality Electronic Design (ISQED) Quality Electronic Design (ISQED), 20th International Symposium on. :216-223 Mar 2019*.

Kanuparhi, A., Karri, R., & Addepalli, S. (2013). Hardware and Embedded Security in the Context of Internet of Things. *CyCAR’13, November 4, 2013, Berlin, Germany*.

Kim, J. (2015). Secure and Efficient Management Architecture for the. *SenSys’15, November 1–4, 2015, Seoul, South Korea.*

Lea, R., & Blackstock, M. (2014). Smart Cities: an IoT-centric Approach. *IWWISS '14, September 01 - 02 2014, Saint Etienne, France*.

Shilton, K., Burke, J., Caffy, K., & Zhang, L. (2016). Anticipating Policy and Social Implications of Named Data Networking. *COMMUNICATIONS OF THE ACM | DECEMBER 2016 | VOL. 59 | NO. 12*.

Speed, C., & Shingleton, D. (2012). An Internet of Cars: Connecting the Flow of Things to People, Artefacts, Environments, and Businesses. *SenseTransport’12, June 29, 2012, Low Wood Bay, Lake District, UK.* .