Machine to Machine Trusted Behaviors

Defining and Implementing Effective and Efficient Trust Mechanisms

Margaret L Loper and Jeffrey D. McCreary
Georgia Tech Research Institute
Atlanta, GA USA
{Margaret.Loper, JD.McCreary}@gtri.gatech.edu

***Abstract*—In the coming decades, we will live in a world surrounded by tens of billions of devices that will interoperate and collaborate in an effort to deliver personalized and autonomic services. Our reliance on these machine-to-machine systems to make decisions on our behalf has profound implications, and makes mechanisms for expressing and reasoning about trust essential. The Georgia Tech Research Institute recently started a strategic initiative on the Internet of Things focusing on trust. We are developing a trust framework for the machine-to-machine domain that classifies leadership functions into three dimensions. We are also developing a live, virtual, constructive platform for the design and validation of trust technologies for fully connected, ubiquitous systems. This work is in an exploratory stage, and our approach and future plans are described in the paper.**

Keywords-Internet of Things; Machine-to-Machine Systems; Trusted Behaviors.

I. INTRODUCTION

The International Telecommunication Union (ITU) predicts that there will be as many as 25 billion devices online within the next decade, outnumbering connected people 6-to-1 [1]. This will lead to a pervasive presence around us of objects and things (e.g., radio-frequency identification tags, sensors, actuators, cameras and mobile phones), which will have some ability to communicate and cooperate to achieve common goals. This paradigm of objects and things ubiquitously surrounding us is called the Internet of Things (IoT). The ITU defines IoT as a "global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies" [2]. The IoT covers different modes of communication, including: between people and things, and between things (Machine-to-Machine or M2M). The former assumes human intervention, and the latter none (or very limited).

A primary aim of IoT is to deliver personalized or even autonomic services by collecting information from and offering control over devices that are embedded in our everyday lives. The reliance of IoT on simple, cheap, networked processors has implications for security; the potentially invasive nature of the information gathered has implications for privacy; and our reliance on machine-to-machine systems to make decisions on our behalf makes mechanisms for expressing and reasoning about trust essential.

While security, privacy and trust are all critical research areas for IoT, our research is focused on trust. The need for trust has long been recognized, as stated recently by Moulds in [3], the "… pivotal role in … decision making means it is essential that we are able to trust what these devices are saying and control what they do. We need to be sure that we are talking to the right thing, that it is operating correctly, that we can believe the things it tells us, that it will do what we tell it to, and that no-one else can interfere along the way."

This work provides an initial concept for trust in the M2M domain. We have completed a seedling phase of this work, which included defining the approach, testbed and use cases, with the detailed work beginning mid-summer. From our exploratory work, our main contributions to trust will be requirements for three dimensions of a trust framework, incorporating leadership functions in these dimensions as would be needed in complex M2M environments, a live virtual constructive research platform for design and evaluation of trust frameworks, and a future focus on cognitive adaptive trust, so that machines learn and recognize situations in which trust should be varied.

The remainder of this paper is organized as follows. In Section II we will define trust and its importance. Section III will briefly describe three dimensions of trust and outline our early work in developing a trust framework. Using intelligent streetlights as a platform for conducting our trust research will be described in Section IV. The remaining two sections will discuss our conclusions and future work.

II. WHY TRUST?

Trust is the belief in the competence of an entity to act dependably, securely and reliably within a specified context [4]. In M2M systems, trust is commonly accomplished using information security technologies, including cryptography, digital signatures, and electronic certificates. This approach establishes and evaluates a trust chain between devices, but it does not tell us anything about the quality of the information being exchanged among machines.

Trust is a broader notion than information security; it includes subjective criteria and experience. Trust is a human belief that someone or something is reliable, good, honest, effective, etc. Trust includes concepts, such as

- Perception – awareness of something through the senses;

- Memory - past history and experience; and
- Context – trust may exist in one situation, but less or not at all in another.

A key challenge is whether the human-to-human concept of trust can be extended to machine-to-machine communication. To make that extrapolation, we must define a way for machines to express and reason about trust. Expressing trust involves defining a rich language for M2M communication, including ontologies to capture the context of the environment. Reasoning about trust must consider the trust chain established among machines, as well as whether the machine is designed for the context in which the trust is required, whether it can accomplish the intended function with the desired results, and whether it has demonstrated a history of reliable performance in the intended function.

Reasoning about trust will vary over time, as machines dynamically join and leave networks. Therefore, the technical theme of our work is to develop a cognitive adaptive trust framework, focusing on core issues of M2M trust in open, decentralized systems with dynamic configuration of networks of objects. The cognitive adaptive aspects of this work are an important long-term goal, but will not be the initial focus of the work.

III. Dimensions of Trust

There are several strategies in the literature that define trust as dimensions. Ahn et al. [5] described the concept of multi-dimensional trust by different agent characteristics, such as quality, reliability and availability. For Matei et al. [6], trust refers to the trustworthiness of a sensor, whether it has been compromised, the quality of data from the sensor, and the network connection. To address behavior uncertainty in agent communities, Pinyol and Sabater-Mir [7] define three levels of trust based on human society: security, institutional and social. Lastly, Leisterm and Schultz [8] identify technical, computational, and behavioral trust, but focus primarily on a behavioral trust indicator.

Our M2M trust framework will focus on three dimensions. These dimensions will work together to create a trusted environment in which machines can independently make decisions on behalf of humans. Our approach to defining trust dimensions is loosely based on the work described in [8] but includes aspects of leadership trust as defined by Covey [9]. This work also has some relationship to Saied et al.'s work [10] in that it considers trust in a heterogeneous IoT architecture involving nodes with different resource capabilities. The dimensions in our framework are described below.

- Technical Trust: establishing and evaluating a trust chain between devices using information security technologies. One way to describe this dimension is integrity - accuracy of algorithms, freedom from virus/malware, machine is operational, and no malfunctions or failures.
- Computational Trust: trustworthy devices that assemble data into actionable information. This dimension covers two qualities: intent and capability. Intent is whether the machine is designed for the context in which the trust is required, and whether it can be tasked with function by other machines. Capability is whether the machine(s) can accomplish the intended function with the desired results, and based on its design, is it suitable for the requesting machine's mission.
- Behavioral Trust: perception of the trustworthiness of information and devices for optimizing the mission performance. In other words, whether the machines demonstrate a history of reliable performance in the intended function.

To illustrate these dimensions, consider the operation of intelligent streetlights (iSL). Intelligent streetlights refer to public street lighting that adapts its behavior based on interactions with pedestrians, cyclists, cars and other environmental conditions. Streetlights can be made intelligent using a variety of sensors to ingest observable data, and networking technology that enables them to behave as a collaborative system. Intelligent streetlights can provide many services, but this example will focus on a simple example of adaptive lighting, where streetlights communicate with their neighbors to create dynamic lighting that follows the presence of pedestrians, bicycles and cars.

If the mission of the intelligent streetlight system is to provide lighting that adjusts based on the presence of humans, all the streetlights in a geographic area must communicate and collaborate to accomplish this mission. Trust in the streetlight system can be broken out across the dimensions as follows:

- Behavioral trust: does the intelligent streetlight system demonstrate a history of reliable performance providing adaptive lighting?
- Computational trust: do the lights turn on in the appropriate area, do they provide adequate light coverage based on speed of the vehicle or pedestrian, and can they predict when someone will reach the next streetlight? Is the light capable of detecting the presence of a vehicle or pedestrian, can it detect the speed they are traveling, can it detect when another light is not working appropriately, and is it capable of changing brightness?
- Technical trust: can the lights be turned on/off, are sensors operating properly, and is there power to operate the system?

This example is intentionally simple to convey the basic ideas of trust dimensions. If the intelligent streetlight system has multiple types of sensors (beyond motion and light) and is tasked to accomplish a variety of missions (e.g., adaptive lighting, rerouting traffic, identifying emergency situations, notifying people about emergency events or evacuations, etc.), then assessing trust along these dimensions becomes more critical.

IV. Intelligent Streetlights as a Platform

In order to conduct our research, we need a problem domain with several key attributes:

- A variety of sensors, devices and machines that allow us to look at machine-to-machine communications;
- The ability for people to interact with the sensors and devices that allow us to look at people-to-machine communications; and
- A problem that can scale to very large numbers of machines and people in order to understand security, privacy and trust as the number of connected systems grows to the hundreds of thousands.

To design and evaluate the M2M trust framework, we will use intelligent streetlights (as described in the previous section) as a demonstration platform. Some initial use cases for evaluating trust include:

- When a pedestrian, cyclist or car is detected, it will communicate this to neighboring streetlights, which will brighten so that people are always surrounded by light.
- When a medical emergency occurs in a crowded area, streetlights can provide communication and location services to medical personnel and responders.
- When an emergency situation occurs in a geographic area, streetlights can notify pedestrians to capture information and evacuate for their personal safety.

The first step in our research will be to develop a simulation of the intelligent streetlight network in order to design and evaluate different algorithms and strategies for security, privacy and trust in fully connected systems. The simulation will be capable of representing large numbers of sensors and machines in order to look at scalability issues related to trust. The second step will be to develop an intelligent streetlight lab on the Georgia Tech (GT) campus. We are targeting a location that provides a variety of behaviors - people walking, sitting in the green space, biking, as well as car traffic. Future expansion of this system could reach further into campus, as well as downtown areas surrounding campus.

Our focus on a simulated and live environment to design and evaluate trust motivates the need for a research platform that can support Live, Virtual and Constructive (LVC) systems. The LVC categorization comes from the distributed simulation community, and refers to the way in which humans interact with simulations. Live involves real people operating real systems for simulated reasons; virtual involves real people operating simulated systems; and constructive involves simulated people (or no people) operating simulated systems [11]. We believe an LVC research platform is key to understanding the interactions and behavior between the physical and virtual world.

The iSL testbed concept is shown in Figure 1. Establishing an outdoor lab will enable us to validate the simulation with actual behavior of the system. This will be important as we begin work on scalability of trust.

The Georgia Tech Research Institute is currently working in different aspects of trust as well as cognitive reasoning, which will be leveraged to support this research. Our expertise in machine learning, modeling and simulation, systems engineering, networking and communications, autonomy, and sensors, will be required to develop the live, virtual and constructive platform to design and test cognitive adaptive trust.

V. Conclusions

Both government and commercial users/providers are trending towards significantly increasing reliance on fully automated complex M2M interactions. Our current work in unmanned systems, cyber, and complex spectrum operations require improved "trust" to achieve their full potential across acquisition/business and operational communities.

To fully realize the desired end state, we must understand the limits of what M2M missions are acceptable; how to visualize and understand trust; and acceptable mission design, execution and degradation parameters. It is also important to explore and validate the role and scope of M2M decision-making or human-in/on-the loop. Ultimately, generating trust in different dimensions will allow decision-makers to confidently invest in and employ M2M, and understand M2M self-optimization.

The work presented in this paper provides an initial concept for trust in the M2M domain. Our main contributions to trust will be well-defined requirements along three dimensions. Understanding the relationship of trust functions to leadership roles will be needed in complex M2M environments. We will also develop a live virtual constructive research platform for design and evaluation of trust frameworks. This LVC environment will connect the physical and virtual worlds, thereby enabling us to define and implement efficient trust mechanisms beyond our demonstration platform. A future focus will be on cognitive adaptive trust, so that machines learn and recognize situations in which trust should be varied.

VI. Future Work

After GTRI demonstrates M2M trust at technical, computational and behavioral levels in simple constructs, the goal is to demonstrate scalability, as well as performance and effectiveness in increasingly complex systems and scenarios. One desired future goal is to demonstrate fully translating and implementing human intent into M2M cognitive adaptive, "creative" execution.

Acknowledgment

We would like to thank the Georgia Tech Research Institute chief scientists for funding this work.

References

[1] International Telecommunication Union, "The State of Broadband: Achieving Digital Inclusion for All," Broadband Commission for Digital Development technical report, September 2012.

[2] International Telecommunication Union, Recommendation ITU-T Y.2060 "Overview of the Internet of Things," June 15, 2012.

[3] R. Moulds, "The internet of things and the role of trust in a connected world," The Guardian, January 23, 2014. Available from: http://www.theguardian.com/media-network/media-network-blog/2014/jan/23/internet-things-trust-connected-world. [retrieved: June 2014]

[4] T. Grandison and M. Sloman, "A survey of trust in internet applications," IEEE Communications Surveys and Tutorials, vol. 3, issue 4, 2000, pp. 2-16.

[5] J. Ahn, D. DeAngelis and S. Barber, "Attitude driven team formation using multi-dimensional trust," Proceedings of the IEEE/WIC/ACM International Conference on Intelligent Agent Technology (IAT '07), Nov. 2007, pp. 229 –235.

[6] I. Matei, J. Baras and T. Jiang, "A composite trust model and its application to collaborative distributed information fusion," Proceedings of the 12th International Conference on Information Fusion (FUSION 2009), July 2009, pp. 1950 –1957.

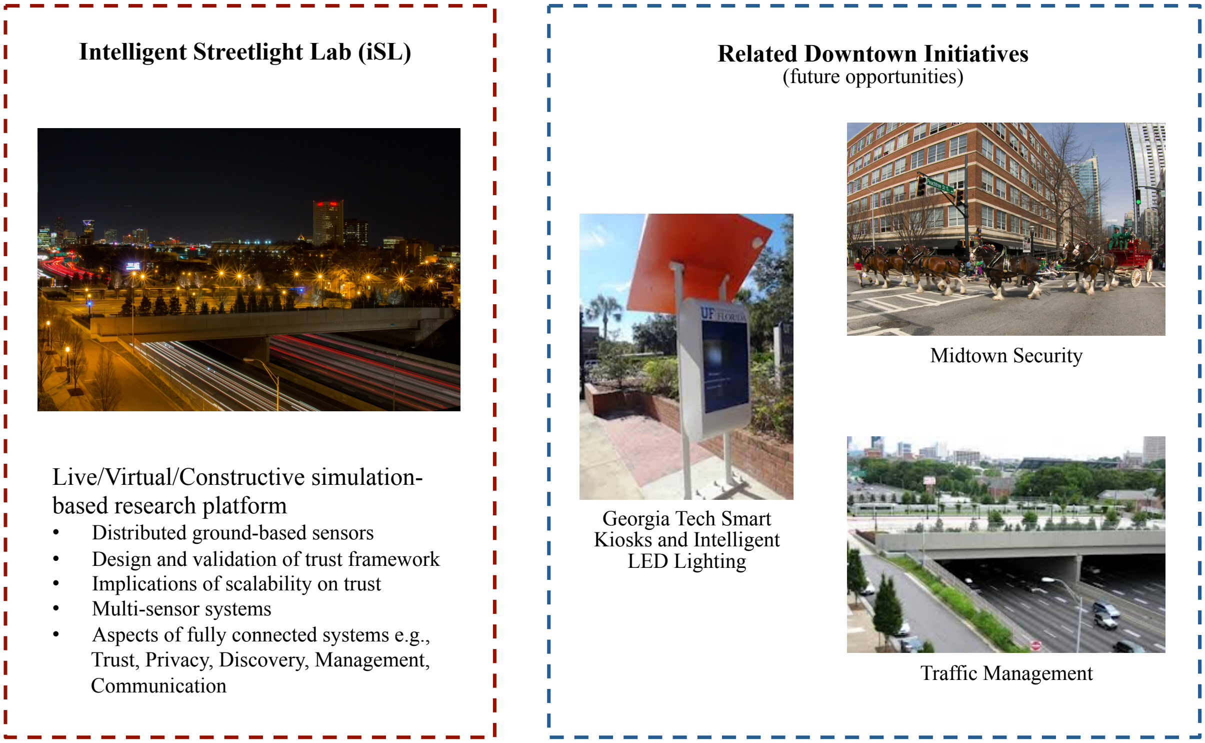
[7] I. Pinyol and L. Sabater-Mir, "Computational trust and reputation models for open multi-agent systems: a review," Artificial Intelligence Review, July 2011, pp. 1–25.

[8] W. Leisterm and T. Schultz, "Ideas for a Trust Indicator in the Internet of Things," Proceedings of the First International Conference on Smart Systems, Devices and Technologies (SMART 2012), IARIA, May 2012, pp. 31-34.

[9] S. Covey, The Speed of Trust, Free Press, 2008.

[10] Y. Saied, A. Olivereau, D. Zeghlache, and M. Laurent, "Trust management system design for the Internet of Things: A context-aware and multi-service approach," Computers & Security, vol. 39 part B, Nov 2013, pp.351-365.

[11] A. Henninger, D. Cutts, M. Loper, R. Lutz, R. Richbourg, R. Saunders, and S. Swensen, "Live Virtual Constructive Architecture Roadmap (LVCAR) Final Report", M&S CO Project No. 06OC-TR-001, Sept 2008. Available from: http://www.msco.mil/LVC.html. [retrieved: June 2014].



Intelligent Streetlight Lab (iSL)

Live/Virtual/Constructive simulation-based research platform

- Distributed ground-based sensors
- Design and validation of trust framework
- Implications of scalability on trust
- Multi-sensor systems
- Aspects of fully connected systems e.g., Trust, Privacy, Discovery, Management, Communication

Related Downtown Initiatives
(future opportunities)

Georgia Tech Smart Kiosks and Intelligent LED Lighting

Midtown Security

Traffic Management

Figure 1. Intelligent Streetlight Laboratory