**Project Title**: Establishing Integrity in Dynamic Networks of Cyber Physical Devices (CNS-0931992, **CNS-0931914**)
**Investigators**: Vinod Ganapathy, Ulrich Kremer (Rutgers University), Trent Jaeger (Penn State)

Dynamic networks allow cyber physical devices to connect opportunistically to share and process data gathered from the physical world. Our project concerns dynamic networks of emerging cyber physical devices, such as smart phones and on-board embedded computing devices, that combine sensors with general-purpose computing environments. These dynamic networks provide a powerful platform of networked devices with significant computation, communication and storage capabilities. However, the opportunistic nature of dynamic networks also raises important security concerns.

Computations in dynamic networks, such as those needed for query processing, may be distributed to several untrusted devices. Some of these devices may be malicious in intent and affect the integrity of computation. It is therefore key to have mechanisms that allow one device to establish the trustworthiness of another device in the dynamic network. Without such mechanisms, devices in a dynamic network may be unwilling to participate or only provide limited access to their resources, which will in turn severely limit the enormous potential of dynamic networks.

In our research, we aim to develop new trust establishment mechanisms for dynamic networks. Existing mechanisms to establish trust, notably techniques based on trusted computing, are not directly applicable to dynamic networks of resource-constrained cyber physical devices. This is because previously proposed trusted computing protocols that allow a prover device to establish its integrity with a verifier device (e.g., IBM's IMA) are interactive and transfer large amounts of data between these devices. These protocols are therefore resource-intensive, both in terms of energy consumption and network bandwidth.

In our work to date, we have conducted an evaluation of the energy consumption of trust establishment protocols for dynamic networks. Using the SARANA dynamic network, and a trusted platform module-enabled machine, we determined that the cost of integrity establishment is substantial. Longer running computations may require multiple integrity measurements, and as such, this cost can dominate the overall cost of both small and large computations.

In a second thread of work, we have been investigating the energy costs of running malware detectors on mobile CPS devices, such as smart phones. Malware detectors allow end-users to establish that these devices are trustworthy, but running a malware detector is a significant source of energy drain. We have conducted a study to formally characterize the security/energy tradeoff of running malware detectors and have identified a sweet spot that provides maximum security while consuming minimum extra energy.