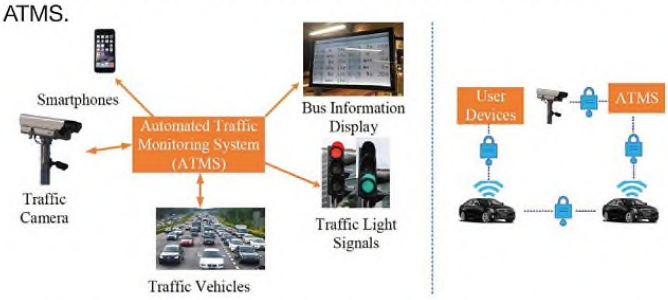
Design Of Light-weight Cyber Security Protocol For Automated Traffic Monitoring Systems

Motivation

Demand for automated vehicles is increasing day-by-day. Driver-less vehicles are requires information from Traffic Monitoring Systems, like speed limit, school zones, road construction, traffic density etc.

Need to replace existing Traffic Monitoring Systems with Automatic Traffic Monitoring Systems (ATMS). ATMS needs to send data securely. Using Public-key Crypto methods requires more resources, hence not advised to use in resource limited ATMS.



Approach: For Low-cost and light weight solutions, using Physically Unclonable Functions (PUFs) for key generation and Authenticated Encryption with Associated Data (AEAD) for encryption and authentication are best solutions.

Project Description

Cyber Security Requirements for ATMS Protocol

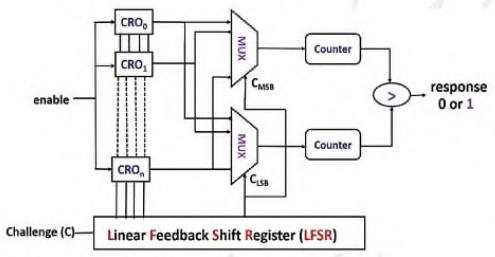
Security: Confidentiality of transmitted and received data. Encryption of transmitted data

Message Integrity: Transmitted data cannot be modified by malicious attacker

Secret Key Generation and Exchange: Key is heart of cryptographic algorithms

Efficiency: Available resources at ATMS traffic sensor side are limited. We have to use light-weight and low cost modules

Physically Unclonable Functions



Components in Proposed ATMS Protocol

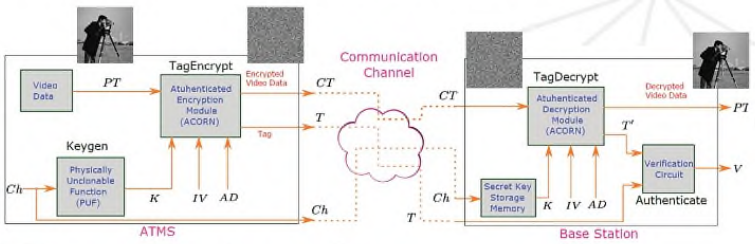
Keygen: Generates the secret key K using the Physically Unclonable Function (PUF). K = Keygen(Ch)

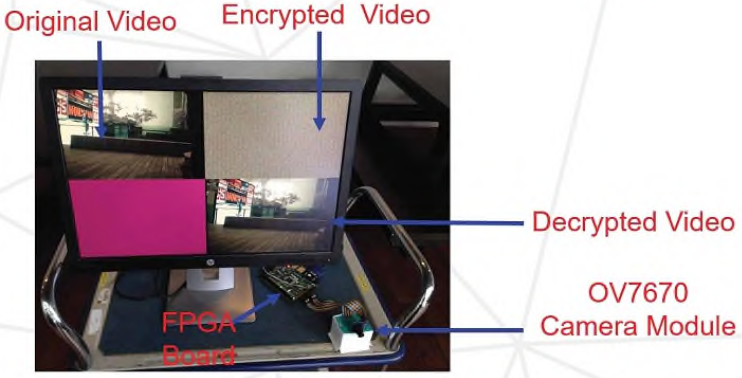
TagEncrypt: Generates encrypted data (CT) and authenticated Tag (T1) from input data (PT) and the secret key (K) using ACORN. ACORN is light-weight AEAD and one of the CAESER competition algorithm (CT, T1) = TagEncrypt(PT, K, IV, AD)

TagDecrypt: Generates the input data (PT) and authenticated tag (T2) from encrypted data (CT) and the secret key (K) using ACORN (PT, T2) = TagDecrypt(CT, K, IV, AD)

Authenticate: Checks for decrypted data same as the original data by comparing both authenticated tags T1 and T2. V = Authenticate (T1,T2); V = 0 means somebody modified the transmitted data

Architecture of Proposed ATMS Cyber Security Protocol





Future Work

The current proposed protocol successfully processed real time videos captured at 640x480 resolution with 30 frame per second. It occupied 8% area of FPGA Nexys 4. In future, we are planning to test our protocol over Wi-Fi, Ethernet and cellular networks.

Sachin Kumar, Vikramkumar Pudi and Anupam Chattopadhyay
School of Computer Science and Engineering
anupam@ntu.edu.sg