Securing Wireless Sensor Networks with Stream Cipher

ErnYu Lee, ShuYun Lim, HoonJae Lee
School of Internet Engineering, Dongseo University
ernyu83@gmail.com, shuyun83@gmail.com, hjlee@dongseo.ac.kr

Abstract

Sensor networks offer economically viable monitoring solutions for a variety of applications. Considerable research has been carried out aiming at providing security primitives for these inexpensive nodes. In order to combat the security threats that sensor networks are exposed to, cryptography protocol is implemented in sensor nodes for point-to-point encryption between nodes. Disclosure, disruption and deception threats can be defeated by authenticating data sources as well as encrypting data in transmission. Given that nodes have limited resources, symmetric cryptography that is proven to be efficient for low-power devices is implemented. Data protection is integrated into a sensor뭡 packet by the means of symmetric encryption with the Dragon stream cipher and incorporating the newly designed Dragon-MAC (Message Authentication Code) authentication protocol. In view that Dragon is a word based stream cipher with a fast key stream generation, it is very suitable for a constrained environment. Our protocol exploited the advantages of link layer security architecture and obtained high security through implementing Dragon symmetric stream cipher in wireless sensor nodes.

1. Introduction

Recent advances in sensor network technology have opens up security challenges in its data transmission over wireless medium. With its wide deployment in hostile environments and security-critical applications, data security and integrity must be well taken care of. Nonetheless, adding security in a resource constrained environment with minimum overhead is a great challenge. Asymmetric encryption and digital signature are claimed to be too expensive to be usable, even symmetric encryption protocol have to be used sparingly.

Related research, TinySec[3] has created efficient link-layer security protocol that is tailored for sensor network. We have based our symmetric stream cipher implementation on this lightweight and generic security package. By looking at the advantages of Dragon[5] stream cipher, we found it to be very suitable to safeguard wireless sensor networks. Dragon is very fast in key stream generation. It is faster than many of its counterparts for instance RC4 in software implementation. Besides, Dragon is able to produce throughputs of gigabits per second in both modern software and hardware. Acting as a fast key stream generator and requires around four kilobytes of memory, it is very appropriate for sensor nodes that have limited code size for application and security.

Besides ensuring data confidentiality, our scheme uses authentication code to achieve two-party authentication and data integrity. Considering that the Dragon state update function (*F function*) is integrated with a high non-linearity virtual S-box; generating a MAC from this design structure can be very competitive in practical applications. Dragon-MAC has retained the structure of Dragon[1] cipher and shared its *F function* for MAC generation. This reversible mapping of 192-bit to 192-bit function is able to supply 4 bytes output that served as a MAC. We hope to introduce this security primitive for achieving a more complete solution for sensor network security.

* This research was supported by South Korean University IT Research Center Project for Mobile Network Security Technology

2. Related Works

Our symmetric encryption scheme relies on TinySec link layer security architecture. Data transfer that relies on carrier sense, which let the nodes detect if other nodes are currently transmitting, are particularly vulnerable to DoS. Link-layer security architecture can prevent this type attack by detecting unauthorized packets when they are first injected into the network, thus putting a stop to energy and bandwidth waste. TinySec support two different security options: Authenticated Encryption and Authentication only. In authentication encryption mode, data payload is encrypted and the entire packet secured by MAC. In contrast, a packet is only secured with MAC in authentication mode thereby decreases the power consumption.

In addition to TinySec, University of California at Berkeley has developed a security building block, SPINS[4], consisting of SNEP to secure point-to-point communication and 킨ESLA for efficient broadcast authentication. SNEP is intended to achieve message confidentiality through encryption. All cryptographic primitives in this scheme are constructed out of a single block cipher for code reuse. RC5 was chosen for Atmega motes due to memory constraints. This block cipher could also serve as a hash function.

While public key cryptosystems is commonly believed to be inefficient for use on low-power devices, BBN Technologies had came out with a solution that can secure sensor networks through Public Key Technology named TinyPK[4]. TinyPK is also known as "Lightweight Security for Wireless Networks of Embedded Systems".