Abstract

With the advent of better health care and medical technology, as well as miniaturized devices with built-in radios, today we can see (WBANs) emerging as one of the main research topics. The sensor nodes worn by patients in a WBAN collect and/or process large amount of data for continuous health monitoring or analysis. However, as the data being dealt with is private and sensitive, even protected by law in many countries, secure data transmission in WBAN is one of key the issues and needs to be addressed before it can be widely deployed. The communication of the sensitive data among the sensors or sensor to health servers give rise to data security concerns like integrity, confidentiality, authentication etc. and the focus of this thesis is to ensure confidentiality of data using encryption, specifically in energy constrained applications as in WBAN.

In this thesis, the energy consumption by 14 of the most popular symmetric ciphers including 11 of the ciphers which are commonly used in lightweight encryption applications have been studied using simulation tool for platform. A new metric called (Metric for Security v/s Energy Consumption) that quantifies the trade-off between energy consumption and security of a cipher has been proposed. In the simulation, the number of CPU cycles have been taken as a measure of energy consumed. It has been shown that the least energy of 0.03 mJ per block is consumed by TEA while LED-64 consumes 2800% (28 times) more energy which is the highest among the investigated ciphers. Taking into consideration the security of these ciphers, the MSEC for these algorithms are -95.56 and -0.615 respectively as their effective key length is very low and can be broken by brute-force. Comparisons show that based on MSEC, AES is the most

optimal cipher with MSEC value of 73.3.

The same suite of algorithms has also been ported on to a hardware mote called TelosB and the energy consumed by the algorithms and their metric value have been measured. We have observed that as TelosB consumes approximately 60% less energy per CPU cycle as compared to MICAz platform. The total energy consumed by ciphers on is lesser than MICAz thus resulting to comparatively higher metric value for TelosB. It has been shown that the least energy of 0.0123 mJ per block is consumed by TEA while LED-64 consumes 2700% (26.9 times) higher. Taking into consideration the security of these ciphers, the MSEC for these algorithms are -97.69 and -0.75 respectively. Comparisons show that based on MSEC, AES is the most optimal cipher on TelosB as well with MSEC value of 73.3. The comparison between the simulation on Avrora for and the actual realization on a hardware mote has shown that the two results are similar.

A deeper study of the lightweight algorithms has also shown that they innovatively mix the various stages of a traditional SPN (Substitution Permutation Network) based cipher like AES. In this thesis, one such new algorithm called LEA (Lightweight Encryption Algorithm) has been proposed which has a skeletal structure similar to AES. The proposed algorithm uses AES S- box for byte-wise substitution and AES key scheduling to generate the round keys. Further, the ShiftRows in AES is replaced by StateTranspose step and a new non-linear step called MixBits has been introduced in this cipher which performs bit-wise operations like bitwise shifts and XOR on the input blocks to increase the diffusion property of the cipher. The MixBits step is analogous to the MixColums step of AES. In addition, for improved security, it uses key whitening as proposed in DESX. Based on observations for DESX, the effective key length of LEA comes down to 191 bits which gives a MSEC value of 154.38 while consuming 0.0219 mJ per block on TelosB platform.

We have observed that as an effect of the MixBits step, LEA has large number of active S-boxes per round and the properties of confusion and diffusion are spread across all the output bytes by end of round 3 of the cipher. In order to perform the preliminary cryptanalysis on LEA, a byte- wise randomness test was conducted for LEA

optimal cipher with MSEC value of 73.3.

The same suite of algorithms has also been ported on to a hardware mote called TelosB and the energy consumed by the algorithms and their metric value have been measured. We have observed that as TelosB consumes approximately 60% less energy per CPU cycle as compared to MICAz platform. The total energy consumed by ciphers on is lesser than MICAz thus resulting to comparatively higher metric value for TelosB. It has been shown that the least energy of 0.0123 mJ per block is consumed by TEA while LED-64 consumes 2700% (26.9 times) higher. Taking into consideration the security of these ciphers, the MSEC for these algorithms are -97.69 and -0.75 respectively. Comparisons show that based on MSEC, AES is the most optimal cipher on TelosB as well with MSEC value of 73.3. The comparison between the simulation on Avrora for and the actual realization on a hardware mote has shown that the two results are similar.

A deeper study of the lightweight algorithms has also shown that they innovatively mix the various stages of a traditional SPN (Substitution Permutation Network) based cipher like AES. In this thesis, one such new algorithm called LEA (Lightweight Encryption Algorithm) has been proposed which has a skeletal structure similar to AES. The proposed algorithm uses AES S- box for byte-wise substitution and AES key scheduling to generate the round keys. Further, the ShiftRows in AES is replaced by StateTranspose step and a new non-linear step called MixBits has been introduced in this cipher which performs bit-wise operations like bitwise shifts and XOR on the input blocks to increase the diffusion property of the cipher. The MixBits step is analogous to the MixColums step of AES. In addition, for improved security, it uses key whitening as proposed in DESX. Based on observations for DESX, the effective key length of LEA comes down to 191 bits which gives a MSEC value of 154.38 while consuming 0.0219 mJ per block on TelosB platform.

We have observed that as an effect of the MixBits step, LEA has large number of active S-boxes per round and the properties of confusion and diffusion are spread across all the output bytes by end of round 3 of the cipher. In order to perform the preliminary cryptanalysis on LEA, a byte- wise randomness test was conducted for LEA

optimal cipher with MSEC value of 73.3.

The same suite of algorithms has also been ported on to a hardware mote called TelosB and the energy consumed by the algorithms and their metric value have been measured. We have observed that as TelosB consumes approximately 60% less energy per CPU cycle as compared to MICAz platform. The total energy consumed by ciphers on is lesser than MICAz thus resulting to comparatively higher metric value for TelosB. It has been shown that the least energy of 0.0123 mJ per block is consumed by TEA while LED-64 consumes 2700% (26.9 times) higher. Taking into consideration the security of these ciphers, the MSEC for these algorithms are -97.69 and -0.75 respectively. Comparisons show that based on MSEC, AES is the most optimal cipher on TelosB as well with MSEC value of 73.3. The comparison between the simulation on Avrora for and the actual realization on a hardware mote has shown that the two results are similar.

A deeper study of the lightweight algorithms has also shown that they innovatively mix the various stages of a traditional SPN (Substitution Permutation Network) based cipher like AES. In this thesis, one such new algorithm called LEA (Lightweight Encryption Algorithm) has been proposed which has a skeletal structure similar to AES. The proposed algorithm uses AES S- box for byte-wise substitution and AES key scheduling to generate the round keys. Further, the ShiftRows in AES is replaced by StateTranspose step and a new non-linear step called MixBits has been introduced in this cipher which performs bit-wise operations like bitwise shifts and XOR on the input blocks to increase the diffusion property of the cipher. The MixBits step is analogous to the MixColums step of AES. In addition, for improved security, it uses key whitening as proposed in DESX. Based on observations for DESX, the effective key length of LEA comes down to 191 bits which gives a MSEC value of 154.38 while consuming 0.0219 mJ per block on TelosB platform.

We have observed that as an effect of the MixBits step, LEA has large number of active S-boxes per round and the properties of confusion and diffusion are spread across all the output bytes by end of round 3 of the cipher. In order to perform the preliminary cryptanalysis on LEA, a byte- wise randomness test was conducted for LEA

on a sample size of 2^{32} in which a very small standard deviation of around 4000 (mean value = 16777216) was observed by end of round 3 indicating that all the possible byte values are spread uniformly across the output block. Also, the energy consumed by LEA is compared with the existing lightweight algorithms and we found that it consumes around 15% more energy than AES but lesser than most other lightweight encryptions proposed in the literature. However the MSEC value of LEA proposed is higher than AES. From the initial cryptanalytic studies, it is possible to conclude that fewer rounds of the proposed algorithm will give rise to better energy efficiency than AES. A detailed cryptanalysis would be needed to provide definitive answer.