The Effect of Symmetric Block Ciphers on WSN Performance and Behavior

Ch. P. Antonopoulos*, Ch. Petropoulos, K. Antonopoulos, V. Triantafyllou, N. S. Voros
Technological Educational Institute of Mesolonghi
Department of Telecommunication Systems and Networks,
National Road Antiriou Nafpaktou, Varia, Nafpaktos 30300, Greece
(*)Corresponding author email: cantonopoulos@teimes.gr

Abstract- **Nowadays Wireless Sensor Networks are increasingly accepted as a reliable solution to highly demanding and critical application scenarios such as military and medical environments, where security support is an absolute prerequisite. However, supporting security implies the execution of cipher algorithms posing significant overheads on WSN nodes, which suffer from scarce resource availability. Moreover, the system wide overheads imposed by requirements related to network performance and behavior are not adequately addressed in current literature. In that direction, this paper intends to evaluate these effects for critical network parameters. The results presented are based on existing results reported in literature measurements concerning the performance overhead imposed by widely utilized encryption algorithms that have been developed for prominent WSN platforms. To evaluate the measurements, the execution performance of three popular cipher algorithms, has been integrated in Omnet++/MiXiM, a well known and widely utilized WSN network simulator. As part of this work, critical insights are provided concerning the system wide effect of deploying security algorithms which are not taken into account when focusing solely in the security algorithm measurements. Furthermore, important trade-offs are provided both qualitatively and quantitatively.**

Keyword: Wireless Sensor Networks, Performance Evaluation, Encryption Algorithms, Security, Privacy and Authentication

I. INTRODUCTION

WSNs are increasingly considered as a mature candidate technology to be utilized in highly sensitive areas such as medical related applications [1]. This is true both for the academic and industrial societies as indicated by the high number of research paper and projects as well as the increasing number of available products.

With respect to sensitive applications, a critical characteristic differentiating them from any other type of applications is the necessity for security support. The data gathered, stored and transferred are governed by strict ethical and legislative regulations concerning their confidentiality. Furthermore, security support pertains to data privacy, data integrity and authentication of communicating parties. The provision of all required features is based on the execution of prominent encryption algorithms, frequently designed and developed in the context of communication technologies with adequate resources. A first critical categorization concern is whether the communicating parties use the same encryption key (i.e. symmetric algorithms using private key encryption) or different (i.e. asymmetric algorithms using public key encryption). With respect to this categorization all relative research efforts converge on the fact that asymmetric cipher algorithms are not a viable solution for WSN environments, due to their high demands on memory and processing time [2][3]. A second categorization is related to the key management approach used from the nodes, in order to agree on the keys to be utilized. Medical applications are characterized by strict ethical regulations concerning privacy and accountability, which favor limited functionality concerning node's entering/exiting the network (i.e. the nodes comprising the network are well defined prior to deployment). Therefore straightforward network wide, group wide or pair wise key approaches can be considered [4].

As it will be presented in the next section, most of the relative research efforts are focusing on enabling the execution of symmetric cipher algorithms on a typical WSN node, as efficiently as possible. However, the work presented in this paper intends to extend respective evaluations to end-to-end communication performance. The latter, usually suffers from unavoidable overheads (which are not related to the implementation efficiency) due to three main reasons: firstly, delay overheads are imposed due to encryption/decryption of the plain text as well as due to the key expansion process; secondly, cipher algorithms are highly intensive from a computational point of view leading to substantial energy consumption each time they are executed; thirdly, in several cases the ciphered data to be transmitted are more than the plaintext data. Such an overhead is, for example, unavoidable when authentication is required since authentication is based on creating a hash code from the whole packet resulting in increased number of bytes to be transmitted.

A typical WSN node comprises of components with extremely limited resources such as low processing capabilities provided by 16Bit based CMUs, limited available memory in the area of 10Kbyte RAM and scarce available energy (most prominent WSN platforms base their operation on few AA batteries). At the same time, WSN nodes are expected to operate unattended from many days to months (for communication intensive applications) or even years (for relaxed communication application scenarios). Finally, WSNs are characterized by the bandwidth which poses significant limitations to the amount of data to be transmitted through the wireless medium.

Consequently, it is easily understood that studying the effect of prominent ciphers on system level network performance and on critical network parameters with varying