UNIVERSIDAD
DE MÁLAGA

Malaga, 7 November 2014

Evaluation of Thesis Proposal

On Automated Evaluation of Key Management Schemes in Wireless Sensor Networks (Filip Jurnecka)

The thesis starts by introducing very briefly the main features of wireless sensor networks, highlighting the hardware limitation of the nodes. It also motivates the need for automatic evaluation of KMS (key management schemes) since manual analysis leads to incomplete evaluation and mistakes. Providing an automated evaluation of KMS is the main goal of the thesis.

Then, the dissertation presents an informal analysis of an existing KMS designed by Delgado-Mohatar et al. The chapter describes a number of naïve security flaws present in the scheme and provides two proposals for amendments. The first one tries to provide truly pairwise keys for nodes since in the original scheme the encryption key of a node is based on a network-wide master key and a random nonce, which the node broadcast to its neighbours. Overall, the first proposal is very close to the well-known LEAP protocol. The second proposal is a combination of the EG random key pre-distribution with a preloaded master key to encrypt the indexes of the keys they own and to establish keys with neighbours with whom they do not have key indexes in common.

Next, the focus is on Key Management Schemes in WSN simulators. It is basically an overview of the state-of-the-art in KMSs for WSNs. First, it briefly reviews some prominent KMS schemes (BROSK, SPINS, PIKE, LEAP and EG) as well as some derivative proposals. Second, it presents a number of properties and metrics, which are useful to evaluate the quality of a particular KMS. Afterwards, it reviews a number of taxonomies and criticise that most of them lack sufficient granularity or present overlapping between categories. Finally, the chapter describes a number of evaluation tools for WSN paying special attention to general purpose and specific WSN simulators. Most of these tools pay no attention to security but the Tuan simulator but it presents some drawbacks such as extensibility and does

not provide information on computational or power consumption. From the number of tools presented, MiXiM is selected for becoming one of the building blocks of the KMS evaluation framework presented in chapter 6. This simulator is selected because it seems to be the most faithful to real WSNs.

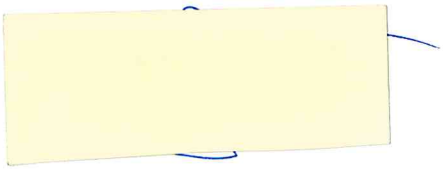
The thesis evolves by showing how to use encryption for authentication. Although the methodology, results and conclusions from this chapter are interesting they do not seem to be much in line with the main focus of the thesis. At least, it seems to me that it is not in the right location within the thesis. As this chapter presents a transformation of the BROSK scheme to provide authentication via encryption, it makes sense to use this transformation as a use case for validating the framework presented in Chapter 6. Even though the transformation is simple, it may have been interesting to see how much this change affects to, e.g., the overall network lifetime.

The following chapter is on the evaluation of Intrusion Detection Systems on Multiple Simulators. It discusses that even though network simulators are a tool of reference for testing protocols, the results they provide for the same (or very similar settings) may differ considerably. The source of differences seems to be caused by implementation mistakes. The simulators used during this research are Castalia, Cooja, MiXiM and WSNet. Due to reliability issues, MiXiM is chosen to build the tool for automated evaluation of KMS properties in WSNs.

Next step is the evaluation of KMS schemes in WSNs. This chapter presents KMSforWSN, a framework for evaluating KMS properties in WSNs. It describes the structure of the framework, the interface every KMS should implement, and the evaluators to each of the KMS properties. A basic library with 5 KMSs has been implemented as well as a universal experiment that can be used as a template for the implementation and evaluation of new KMSs. Some features not considered in the experiment include the mobility, battery depletion of nodes and the presence of a base station in the network, but the candidate claims that it will be possible to consider these features. The candidate also wonders whether it is worth considering a node capture attack other than a random strategy. This is discussed in detail in the following chapter. Finally, there is an extensive body of research on the (automatic) validation of security protocols: model checkers, symbolic search, theorem proving, pi-calculus,...

The final chapter deals with node capturing attacker strategies, and examines how much KMSs are affected by the movement pattern of an adversary performing node capture attacks. Besides the typical random attacker model, three other strategies are developed. The new strategies consider that an attacker might capture nodes at the border, while moving between two points or at a certain location. After evaluation of the various strategies in multiple scenarios with 3 KMSs and different parameters it seems that the outermost strategy is the worst strategy and the centre drop strategy being slightly better than the rest. Finally, the chapter presents the evaluation of some other metrics for the previous KMSs, namely, connectivity, memory requirements and code size.

From all the above, I conclude that the thesis properly addresses the problem initially formulated. The candidate has shown a good knowledge of the general background, and the research problem has been defined and put into perspective. The final results are relevant for the current research field. Therefore, I recommend the PhD to be awarded with grade B, and in case of unconvincing defence, I also find grade C acceptable.



Javier Lopez, Professor
University of Malaga, Spain