Demo: Security Mechanisms Impact and Feasibility on Wireless Sensor Networks Applications

Cíntia B. Margi*, Bruno T. de Oliveira*, Gustavo T. de Sousa*, Marcos A. Simplicio Jr†,
Flávio H. Freitas†, Paulo S. L. M. Barreto†, Tereza C. M. B. Carvalho†, Mats Näslund‡ and Richard Gold‡
* Escola de Artes, Ciências e Humanidades (EACH)
Universidade de São Paulo (USP) – Brazil
Email: {cintia,brunotrevizan,gustavot}@usp.br
† Departamento de Engenharia de Computação e Sistemas Digitais (PCS)
Escola Politécnica da Universidade de São Paulo (EPUSP) – Brazil
Email: {mjunior,ffreitas,pbarreto,carvalho}@larc.usp.br
‡ Ericsson Research
SE-16480 Stockholm – Sweden
Email: {mats.naslund,richard.gold}@ericsson.com

***Abstract*— The deployment of security solutions in Wireless Sensor Networks (WSNs) is considered a challenge due to the highly constrained devices involved in these applications. However, due the need for security services such as confidentiality, integrity and authenticity in a large number of important scenarios, such mechanisms are made necessary. In this demonstration paper, we show that deployment of security algorithms on a WSN testbed is possible without causing significant impact on the performance of such applications.**

I. Introduction and Background

Most WSN deployments do not consider security among their requirements. However, when targeting WSN for health applications or scenarios that monitor sensitive information, it is important to deploy confidentiality mechanisms. Furthermore, data integrity and authenticity are critical in order to prevent fake data that could lead to mistaken actions. Therefore, it becomes necessary to employ security mechanisms such as encryption algorithms and Message Authentication Codes (MACs) to provide confidentiality, integrity and authenticity in such scenarios. In order to use these algorithms, applications need to deal with the distribution of secret keys, which is a complex issue in these environments [8].

Law et al. [4] present a survey and benchmark of block ciphers that could be used in sensor networks, and choose AES [2] and Skipjack [5] for scenarios with, respectively, high and low security requirements. However, implementing regular algorithms and protocols that account for security is a difficult problem in such constrained environments. Hence, the drawback on using non-specific WSNs cipher algorithms usually is that one has to choose performance over security level or vice-versa.

Security is often (and sadly) considered at the very last step in system design. Therefore, security tends to be looked at purely as an "extra cost" due to the execution/energy overhead it appears to add to the system. In this work, we show that security algorithms, such as encryption algorithms (namely Curupira) and Message Authentication Code (MAC) algorithms (namely Marvin) do not impact WSN applications significantly and can be used in WSNs.

Curupira [7] is a special-purpose block cipher tailored for constrained platforms, which takes 96-bit blocks organized as 3×4 byte matrices. It accepts 96-, 144- or 192-bit keys and takes, respectively, 10, 14 or 18 rounds for its operation. Such as AES, this cipher also follows the Wide Trail Strategy and, thus, has a similar round structure built from four transformations: a Nonlinear Layerγ, in which all bytes in the block pass through a highly nonlinear S-Box; a Permutation Layer π, in which all the bytes in the second and third rows of the block are permuted to provide inter-columns diffusion; a Linear Diffusion Layer θ, in which the block is left-multiplied by an MDS matrix; and a Key addition Layer σ, in which the round key is XORed with the block. Curupira accepts two versions for its key schedule. In the more conservative Curupira-1, the key schedule structure is also based on the Wide Trail Strategy, while it takes the form of a linear feedback shift register in the Curupira-2.

The deployment of efficient Message Authentication Codes (MACs) is also an important issue in sensor networks. A reasonable strategy in such constrained scenarios is to adopt a cipher-based MAC, reducing the memory requirements for the MAC algorithm itself. Marvin [6] algorithm was especially developed with constrained platforms in mind. It follows the ALRED construction, providing a trade-off for iterated block ciphers that process data blocks in chunks of fixed length. The Marvin structure closely follows the randomize-then-combine paradigm, adopting a variant of Krawczyk's $h_p(M)$ cryptographic CRC to generate secret offsets. These offsets are then combined with the message blocks by means of the so called *Square Complete Transform*, which corresponds to 4 unkeyed rounds of the underlying block cipher when this cipher belongs to the Square family.

II. The Wireless Sensor Network Security Demonstration

This demo testbed is composed by Crossbow TelosB [1] motes running Contiki 2.2.1 OS [3]. This sensor node is a low power IEEE802.15.4 compliant wireless platform, which includes off-the-shelf temperature, humidity, light and infra-red light sensors, as well as a 16-bit 8MHz Texas Instruments micro-controller with 10Kbytes of RAM and 48Kbytes of Flash memory.

In order to show that security that algorithms do not impact WSN applications significantly and can be used in such scenarios, we create four WSNs, each of which has two nodes. The first WSN transmits and decodes received plain packets (i.e., no security mechanisms are used). The second WSN works with authenticated packets using Marvin, while the third one encrypts data with Curupira. The fourth one combines data encryption and authentication, using both Curupira and Marvin. Furthermore, as shown in Figure 1, there is also a spy node that monitors all data being transmitted by these networks.

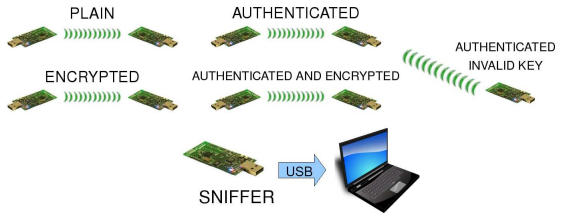

Fig. 1. Demonstration testbed setup.

The data captured by the spy node, who is attached to a laptop through the USB port, is displayed in a console on the laptop. The spy node can understand both the data transmitted through the insecure network and the data from the authenticated network, but it will not understand data exchanged in the encrypted and encrypted/authenticated WSNs. Then we will be able to show that we can achieve confidentiality without performance loss.

Data packets have 12 bytes in the plain insecure network, as well as on the encrypted data network. On the other hand, data packets have 16 bytes on both the authenticated and encrypted/authenticated networks due to the addition of the authentication tag.

Given that all nodes are in range, receivers in all four networks will sense data from the other three networks. Since the networks operate with different data packet format, a packet from the encrypted/authenticated network may cause errors in the insecure network, and so on. In order to show if a packet is compliant to a given network or if it causes some kind of error, we will use the sensors' LEDs. When the message format is as expected and the data value is acceptable, the green LED will turn on; conversely, the red LED will light if network message format is invalid or if a non-authenticated message is received (when an authenticated one was expected). If the message format is as expected and the authentication tag (if required) is valid, but an unexpected value is received, the blue LED will light.

Table I summarizes which LEDs will turn on when data is received in a given network. Notice that with this combination of networks and types of data being transmitted/received, we were able to show the behavior of different levels of network security.

TABLE I

LEDs behavior for a given network and type of data received.

	Network			
Data	Plain	Encrypted	Authenticated	Enc/Auth
Plain	Green	Blue	Red	Red
Encrypted	Blue	Green	Red	Red
Authenticated	Red	Red	Green	Blue
Enc/Auth	Red	Red	Blue	Green

The process to transmit data (and encrypt/authenticate if needed) will be triggered by pushing one of the TelosB buttons. Just before transmitting data, a LED will turn on. On the receiving node, after data is received and processed, the status LED will turn on. So one will be able to observe that all four networks run at almost the same speed.

The last step showed on this demo is data authentication validation. Another node will send authenticated data, using the correct packet format, but using an invalid key. Nodes on the authenticated network will verify that the authentication tag is invalid.

III. Conclusions and Future Work

In this work, we demonstrated that security mechanisms can be implemented on the Wireless Sensor Network (WSN) without incurring in significant overhead. We are currently working on hardware and OS interoperability issues, and soon we will add MicaZ/TinyOS nodes to our testbed. Moreover, we continue the performance evaluation of security mechanisms.

IV. Acknowledgements

This work was supported by the Research and Development Centre, Ericsson Telecomunicações S.A., Brazil.

References

[1] Crossbow. Telosb datasheet. `http://www.xbow.com/Products/Product_pdf_files/Wireless_pdf/TelosB_Datasheet.pdf`, 2008.

[2] J. Daemen and V. Rijmen. *The Design of Rijndael: AES – The Advanced Encryption Standard*. Springer, Heidelberg, Germany, 2002.

[3] A. Dunkels, B. Grönvall, and T. Voigt. Contiki - a lightweight and flexible operating system for tiny networked sensors. In *Proc. of the First IEEE Workshop on Embedded Networked Sensors (Emnets-I)*, Nov. 2004.

[4] Y. W. Law, J. Doumen, and P. Hartel. Survey and benchmark of block ciphers for wireless sensor networks. *ACM Trans. Sen. Netw.*, 2(1):65–93, 2006.

[5] NSA. *Skipjack and KEA Algorithm Specifications, v2.0*. National Security Agency, 1998.

[6] M. Simplicio, P. Barbuda, P. Barreto, T. Carvalho, and C. Margi. The marvin message authentication code and the lettersoup authenticated encryption scheme. *Security and Communication Networks*, To appear in 2009.

[7] M. Simplicio, P. Barreto, T. Carvalho, C. Margi, and M. Näslund. The Curupira-2 block cipher for constrained platforms: Specification and benchmarking. In *Proc. of the 1st International Workshop on Privacy in Location-Based Applications - 13th European Symposium on Research in Computer Security (ESORICS'2008)*, volume 397. CEUR-WS, 2008.

[8] Y. Xiao, V. K. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway. A survey of key management schemes in wireless sensor networks. *Computer Communication*, 30(11-12):2314–2341, 2007.