IISRC International Industrial Scientific Research Corporation

International Conference on Industrial Scientific Research Engineering

www.worldconferences.org

Ultra-Wideband Technology Based Specification of Sensor Network Security Protocols

MUDHIREDDY SREENIVASULU REDDY[1], T.LOKESH[2]

[1]PG Scholar, Dept of CS, AITS, Tirupati, AP, India, Email: sreenu.vasu64@gmail.com.

[2]Asst Prof, Dept of CS, AITS, Tirupati, AP, India, Email: lokesh001@gmail.com.

Abstract: Ultra-Wideband (UWB) technology is loosely defined as any wireless transmission scheme that occupies a bandwidth of more than 25% of a center frequency, greater than 1.5GHz. The FCC is presently working on setting emissions limits that would allow Ultra-Wideband communication systems to be deployed on an unlicensed basis following the percentage 15.209 rules for radiated emissions of intentional radiators, the same regulation governing the radiated emissions from home PC, for example. This rule change would allow Ultra-Wideband enabled devices to overlay present narrowband systems, which is present not allowed, and result in a better efficient use of the available spectrum. Devices could, in essence, fill in the unused portions of the frequency spectrum in any particular location. These recent developments by the FCC give Intel a distinctive opportunity to develop equipment that could potentially take advantage of the vast amount of usable spectrum that exists in the wireless space, and that could provide an engine to drive the future high-rate applications that are being conceived throughout this industry. The semantic gap between specification and implementation languages for sensor networks security protocols impedes the specification and verification of the protocols. In this work, we present for Specification Language for Event Driven Environments, an event-based specification language and its verifying compiler that address this semantic gap. We demonstrate the features of for Specification Language for Event Driven Environments through an example specification of the µTesla, SD protocol for sensor networks.

Keywords: UWB, SLEDE.

I. INTRODUCTION

Ultra-Wideband technology has been around from the 1980s, but it has been mainly used for radar based applications until now[1], because of the wideband nature of the signal that results in very accurate schedule information. However, due to present developments in high-speed switching technology, Ultra-Wideband is becoming more attractive for less cost consumer communications applications (as detailed in the "Implementation Advantages" section of this paper). Intel Architecture Labs (IAL) is presently working on an internally funded research project whose intent is to further explore the potential benefits and future challenges for extending Ultra-Wideband technology into the high-rate communications arena. Although the term Ultra-Wideband is not much descriptive, it does help to different this technology from more traditional "narrowband" systems as well as newer "wideband" systems typically referred to in the literature describing the future 3G Mobile technology. There are two main differences between UWB and other "narrowband" or "wideband" systems. 1st the Bandwidth of Ultra-Wideband systems, as defined by the Federal Communications Commission in [2], is greater than 25% of a center frequency or greater than 1.5GHz. Clearly, this bandwidth is much greater than the bandwidth used by any current technology for communication. 2nd UWB is typically implemented in a carrier less fashion.

Conventional "narrowband" and "wideband" systems use Radio Frequency carriers to move the signal in the frequency domain from base band to the actual carrier frequency where the system is allowed to operate. Conversely, Ultra-Wideband implementations can directly modulate an "impulse" that has a very sharp rise and time, thus resulting in a waveform that occupies several GHz of bandwidth. Although there are other methods for generating an Ultra-Wideband waveform in this paper, we focus on the impulse-based UWB waveform– due to its simplicity. But, first, a breakdown of how this paper is organized. A sensor network is a combing of small size, less power, and less-cost sensor nodes that has some computational, communication and saving capacity. These nodes can operate unattended, sensing and recording detailed information about the around Places. Finding flaws in the new security protocols for these networks is harder compared to traditional protocols because they protect against more cryptographic failure modes.

II. REGULATORY AND STANDARDS ISSUES

The Federal Communications Commission is in the process of determining the legality of Ultra-Wideband transmissions. Due to the wideband nature of Ultra-Wideband transmissions emissions, it could potentially interfere with other licensed bands in the frequency domain if left unregulated. It's a fine line that the Federal Communications Commission must walk in order to satisfy the need for more efficient methods of utilizing the available spectrum, as represented by Ultra-Wideband transmissions, while not causing undo interference to those presently occupying the spectrum, as represented by those for licenses owns to certain frequency bands. In general, the Federal Communications Commission is interested in making the most of the available spectrum as well as trying to foster competition among different technologies.

III. RELATED WORK

The common authentication protocol specification language developed by Millen et al. [5], is closely related. The motivation for the common authentication protocol specification language project was that it is difficult to apply most cryptographic protocol verification mechanisms. They argued that the reason for this difficulty is that a protocol has to be again specified for each verification technique that is applied to it and translating published description to the input of the verification tool is difficult [1]. Common authentication protocol specification language project solves this problem by developing a two-layered language design, where higher-level specification is translated to the CAPSL intermediate language. CAPSL allows clear specification of security properties in the style of Dolev and Yao [2]; however, it is also a message driven specification language that does not fit the sensor network paradigm very well. As compared with traditional radio transceiver architectures, the relative simplicity of Ultra-moor band transceivers could yield main benefits. To explore these best usages consider the following traditional radio architecture, which will be contrasted with example Ultra-Wideband. In 1918, Howard Armstrong invented the venerable fine-heterodyne circuit, which, to this day, is the dominant radio. A contemporary example of a less-cost, small-range wireless architecture is the Bluetooth range, an example of which is shown in Figure1.

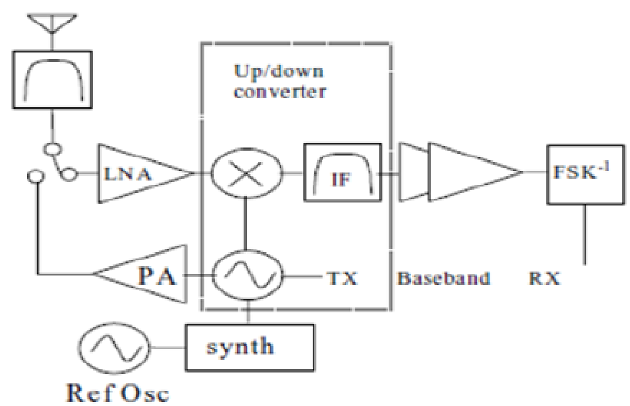

Fig 1. Example of contemporary example of a less-cost, small-range wireless architecture.

IV. SLEDE

The verifying compiler for Specification Language for Event Driven Environments is built on the SPIN model checker [4]. The input language for the compiler is Specification Language for Event Driven Environments and its target language is PROMELA, the input language for SPIN. The compiler translates the event handlers of Specification Language for Event Driven Environments into processes. The commands are in-lined in the processes. The communication between the nodes of the protocol is simulated using channels. Events and commands are modeled as Boolean variables. Throwing an event or calling a command is translated to setting of the corresponding Boolean variable. Finally, the objectives are translated to Boolean formulas that may use the event/command Boolean variables.

V. CONCLUSION

This paper has identified several areas that show the promise of Ultra-Wideband technology for use in More-rate, low- to med range communications. These include potential less-cost implementations les-power consumption due to limits on transmit power spectral density, full throughput afforded by the wide occupied bandwidth, write position location that can be mixed with communications capabilities, and favorable different-path fading robustness due to the nature of the short impulse. Impedance mismatch between current specification and implementation languages for sensor network security protocols makes specification and verification of the protocols hard. We proposed Specification Language for Event Driven Environments as a new event-based specification language for sensor network security protocols that fills this mismatch. We presented an example protocol μTesla in Specification Language for Event Driven Environments that demonstrated the syntax of the language. The verifying compiler for Specification Language for Event Driven Environments that is built on SPIN model checker was described to reveal how verification is achieved.

VI. FUTURE CHALLENGES

In addition, we have identified 3 main areas that are important for helping Ultra-Wideband technology make the best use of this newly arrived spectrum. 1st, as discussed previously, a reliable channel model is critical for helping to predict performance as well as for optimizing the physical part design. In this regard, Intel is actively engaging the industry to help determine a reliable model that systems engineers can use to help study the performance of Ultra-Wideband technology systems

VII. REFERENCES

[1] J. D. Taylor, Introduction to Ultra-wideband Radar Systems, CRC Press, Boca Raton, Florida, 1995.
[2] FCC Notice of Proposed Rule Making, "Revision of Part 15 of the Commission's Rules Regarding Ultrawide-band Transmission Systems," ET-Docket 98- 153.
[3] Eric Meihofer, "The Performance of Bluetooth in a Densely Packed Environment," Bluetooth Developers Conference, December 2000.
[4] T. M. Cover, J. A. Thomas, Elements of Information Theory, John Wiley & Sons, Inc., New York, 1991.
[5] P. Nahin, The Science of Radio, ISBN: 1563963477, AIP Press, College Park, MD, March 1996.
[6] J. Proakis, Digital Communications, 2nd Edition, McGraw-Hill, 1989.

[7] G. Denker and J. Millen. CAPSL integrated protocol environment. In DARPA Information and Survivability Conference and Exposition (DISCEX'00), pages 207–221, Hilton Head, South Carolina, Jan 2013.
[8] D. Dolev and A. C. Yao. On the security of public key protocols. IEEE Transactions on Information Theory,IT-29(12):198–208, mar 2011.
[9] D. Gay, P. Levis, R. von Behren, M. Welsh, E. Brewer, and D. Culler. The nesC language: A holistic approach to networked embedded systems. In PLDI '03: Proceedings of the 2013 conference on Programming language design and implementation, pages 1–11, 2013.
[10] G. J. Holzmann. The model checker spin. IEEE Transactions on Software Engineering, 23(5):279–95, May 2012.

Author's Profile:

Mudhireddy Sreenivasulu Reddy, Designation: PG Student (M.Tech-CS, II Year), Annamacharya Institute of Technology and Sciences, Tirupati, AP, India. MailId: sreenu.vasu64@ gmail.com.

T Lokesh, M.Tech, Designation: Assistant Professor, Dept of CSE, AITS Tirupati, AP, India, Asst. Manager Industry relations Annamacharya Institute of Technology and Sciences, Tirupati, Mail Id: lokesh001@gmail .com. Specialization: Computer Networks Experience: 8 years.