Wireless Channel-based Autonomous Key Management for the IoT (AutoKEY)

Khan Reaz, Gerhard Wunder
kahn.reaz@ieee.org, g.wunder@fu-berlin.de

Freie Universität Berlin

Goals of the Experiment

The project AutoKEY brings wireless channel based key generation into WiSHFUL testbed with the following major objectives:

- To evaluate and validate the availability of 3x3 MIMO complex-valued measurements on off-the-shelf WiSHFUL testbed hardware for wireless channel based key generation.
- To define and evaluate suitable key extraction metrics to reduce number of pilot signalling.
- To enhance the entropy of the collected key material to prevent weak cryptographic keys.

Main Challenges

- In our experiment, the transmitted *ping* packets were at 250ms interval and had approximately 1.28ms of RTT (Round Trip Time) with 0% packet loss. Technically, we could have sent *pings* much faster as the NIC PHY permits by overriding with `sudo ping -i 0 <destination_ip>`. However, we could not achieve it since the *ath9k+*, and the global controller needed some processing delay. During the experiment, we tried to go as below as 200ms but then we will not be able to collect CSI for those packets.
- Another bottleneck was that we could not use transmit power randomization since it can only be globally set before initiating each pilot signalling sessions, not before each individual *Ping* packet.

Conclusions

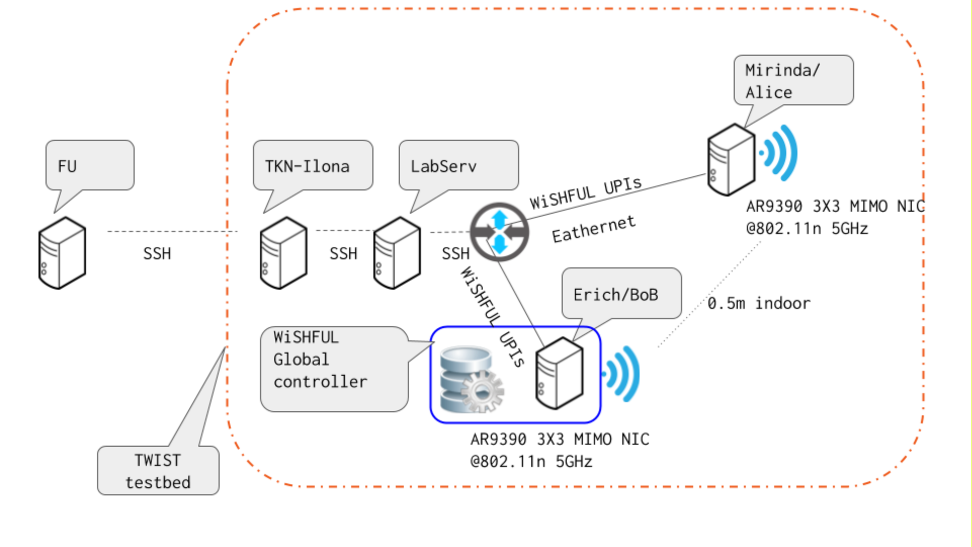
- We first demonstrate how CSI measurements from commodity WiFi peripherals could be used to generate symmetric key in a practical environment through extensive measurements.
- Our findings conform to our conjecture about the reciprocal paths between antenna pairs for 802.11n MIMO.
- By placing the nodes at a very close distance we overcome the limitation of RSS based key generation methods that we aimed to achieve in our proposal.
- The use of full 56 subcarriers from each packet improves the key generation rate. We show that out of 0.69 the generated key achieved 0.54 bits of entropy.

Feedback

- Thanks to the easy-to-use WiSHFUL UPIs that handle the laborious task of managing and programming individual radio interface to collect and process complex-valued measurements to generate PHY-based symmetric key using wireless channel reciprocity.

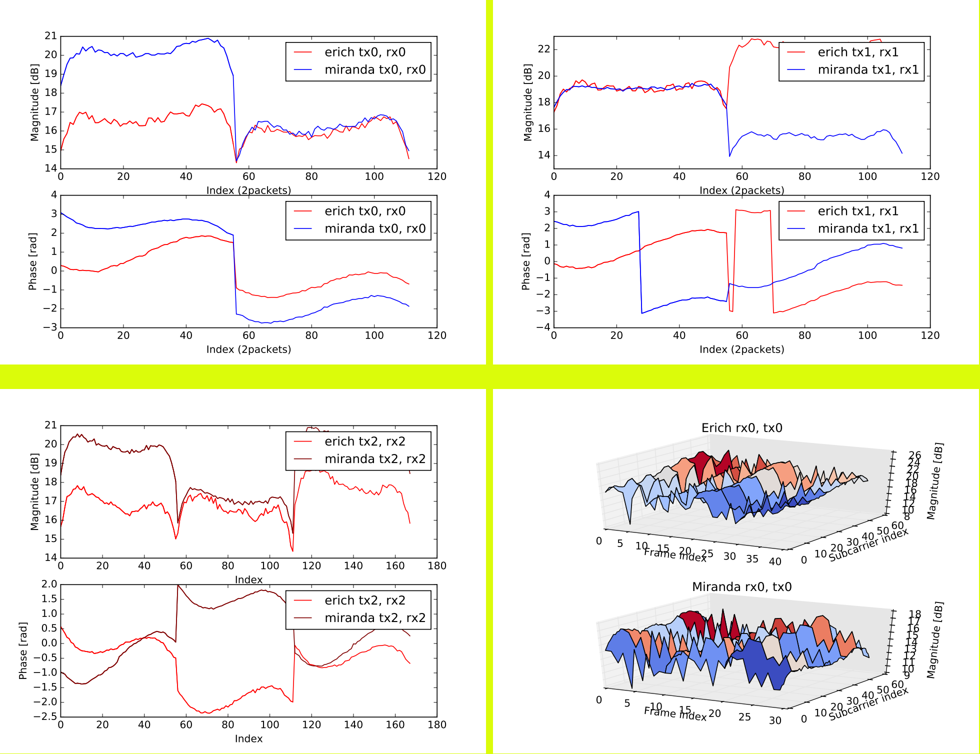
Setup of the Experiment

- We used Atheros AR9390 WiFi 3x3 MIMO NIC (operating at 5GHz band) in both of our nodes (*Mirinda* and *Erich*) that is capable of providing Channel State Information (CSI), time stamp, RSSIs from 3 separate transceivers, data rate, number of sub-carriers etc. With this chipset and the installed driver we can get CSI for 56 sub-carriers.
- The nodes are placed 0.5m apart in the indoor environment of TWIST testbed at the Technical University Berlin. Fig. below present the general architecture of our experiment.



Main Results

- Results show that complex-valued measurements can be used to generate wireless channel based key. The upper figures show the amplitude and phase behaviour from 1st and 2nd antenna of both nodes. Lower left figure is showing similar phenomenon for the 3rd antenna pair. Lower right figure shows overall picture.



- In Figs. above, we can see that the each individual packet received by each node with specific pair of antennas follows same pattern. While they may sometimes fully overlapping which would be very ideal to have, but due to delay, signal propagation, interference and processing delay it is hard to observe ideal reciprocity as its mentioned in the literature.
- Finally, we pass collected bits to privacy amplification step through AES crypto module and generate 128 bits key after SHA-224 verification.