CISTER
Research Centre in
Real-Time & Embedded
Computing Systems

Poster

Cooperative Key Generation For Data Dissemination in Cyber-Physical Systems

Kai Li
Harrison Kurunathan
Ricardo Severino
Eduardo Tovar

CISTER-TR-180207

2018/04/10

Cooperative Key Generation For Data Dissemination in Cyber-Physical Systems

Kai Li, Harrison Kurunathan, Ricardo Severino, Eduardo Tovar

*CISTER Research Centre

Polytechnic Institute of Porto (ISEP-IPP)

Rua Dr. António Bernardino de Almeida, 431

4200-072 Porto

Portugal

Tel.: +351.22.8340509, Fax: +351.22.8321159

E-mail: kaili@isep.ipp.pt, hhkur@isep.ipp.pt, rar@isep.ipp.pt, emt@isep.ipp.pt

http://www.cister.isep.ipp.pt

Abstract

Securing wireless communication is significant for privacy and confidentiality of sensing data in Cyber-Physical Systems (CPS). However, due to broadcast nature of radio channels, disseminating sensory data is vulnerable to eavesdropping and message modification. Generating secret keys by extracting the shared randomness in a wireless fading channel is a promising way to improve the communication security. In this poster, we present a novel secret key generation protocol for securing real-time data dissemination in CPS, where the sensor nodes cooperatively generate a shared key by estimating the quantized fading channel randomness. A 2-hop wireless sensor network testbed is built and preliminary experimental results show that the quantization intervals and distance between the nodes lead to a secret bit mismatch.

Cooperative Key Generation For Data Dissemination in Cyber-Physical Systems

Kai Li, Harrison Kurunathan, Ricardo Severino, and Eduardo Tovar
Real-Time and Embedded Computing Systems Research Centre (CISTER), Porto, Portugal.
E-mail:{kaili,hhkur,rarss,emt}@isep.ipp.pt

***Abstract*—Securing wireless communication is significant for privacy and confidentiality of sensing data in Cyber-Physical Systems (CPS). However, due to broadcast nature of radio channels, disseminating sensory data is vulnerable to eavesdropping and message modification. Generating secret keys by extracting the shared randomness in a wireless fading channel is a promising way to improve the communication security. In this poster, we present a novel secret key generation protocol for securing real-time data dissemination in CPS, where the sensor nodes cooperatively generate a shared key by estimating the quantized fading channel randomness. A 2-hop wireless sensor network testbed is built and preliminary experimental results show that the quantization intervals and distance between the nodes lead to a secret bit mismatch.**

***Index Terms*—Data dissemination, Cyber-Physical Systems, Wireless security, Experimental evaluation**

I. Motivation

Real-time data dissemination provides a fundamental distribution service for many applications in Cyber Physical Systems (CPS), e.g., vehicular platoons [1], intelligent transportation systems [2], wireless sensor-actuator networks [3], and Internet of Things [4]. Due to broadcast nature of radio channels, disseminating sensory data is vulnerable to eavesdropping, and message modification from an illegitimate eavesdropper. To improve communication security in CPS, using a shared secret key for data encryption/decryption is crucial to support data confidentiality, integrity, and sender authentication. Key generation based on the randomness in a wireless fading channel is a promising approach [5], where two sensor nodes extract secret bits from the inherently random spatial and temporal variations of the reciprocal wireless channel between them. However, previous works on fading channel based secret key generation mainly focused on improving the secret bit generation rate between a pair of sensor nodes (by exploiting temporal and spatial variations of radio channel, multiple antenna diversity, or multiple frequencies). The problem of unanimity of the generated key for the real-time data dissemination remains as a challenge.

In this poster, we present a new data dissemination security protocol that quantizes the estimated received signal strength (RSS) measurements. The quantization intervals are cooperatively adapted to reduce secret bit mismatch rate (BMR). Note that the secret key generated by our protocol is based on channel randomness over multiple hops, the eavesdropper at a different location experiences independent channel fading, which is not able to obtain the same key. In addition, the proposed protocol can be applied to more critical systems, as the secret key is generated in a distributed manner, eliminating single point of failure.

A 2-hop Wireless Sensor Network (WSN) testbed is built to empirically study the performance of our protocol. The results are significant because they provide invaluable information for improving the wireless security and key generation in future research.

II. Cooperative Secret Key Generation

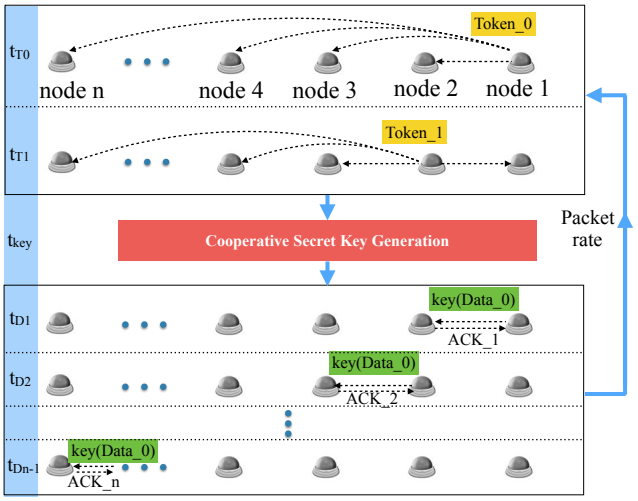

Fig. 1: The secure data dissemination in the CPS that contains n nodes.

We consider n nodes of interest in the network, forming $(n-1)$ wireless hops, as shown in Fig. 1. Without loss of generality, it is assumed that route from the source node to the sink node has been constructed by routing protocols. At time t_{T0}, the data source, i.e., node 1, broadcasts a token packet Token_0, which contains node ID and timestamp. Once Token_0 is successfully received by the node 2, node 2 sends the Token_1 at t_{T1}, which which is also an acknowledgement to Token_0. According to reception of the Token_0 and Token_1, node i $(i \in [3, n])$ is aware of the channel quality with the node 1 and 2, which are denoted by $H_{i,1}$ and $H_{i,2}$. Moreover, the receiving power

at node i (denoted by P_i^{rx}) can be specified by

$$P_i^{rx}(\text{dB}) = P_j^{tx}(\text{dB}) + K_1 + K_2 - 10\eta_{PL}\log_{10}(d_{i,j}) + \phi_{i,j} \quad (1)$$

where P_j^{tx} is the transmit power of node j ($j = 1, 2$). K_1 and K_2 are positive fixed constants relating to the channel. The term $\phi_{i,j}$ denotes background noise power of the link, which is independent fading over different time epochs. In addition, $H_{i,j} = (P_j^{tx} - P_i^{rx})$ presents the channel gain of the link between sender node j and receiver node i. Since the channel randomness information cannot be transmitted over the public channel that is observable to the eavesdropper, based on (1), the channel quality between node 1 and 2 is estimated by node i using $\tilde{H}_{1,2}^i = H_{i,1} - H_{i,2}$.

Next, let ξ_q and Q denote the q-th quantization interval and the total number of quantization intervals, respectively, where $q \in [1, Q]$. The probability that the secret key of all the nodes is unanimous defines $\mathcal{P}(\mathcal{L}(\tilde{H}_{1,2}^i) \in [\xi_q, \xi_{q+1}])$, where $\mathcal{L}(\tilde{H}_{1,2}^i)$ is the quantized $\tilde{H}_{1,2}^i$ at node i ($i \in [3, n]$). Thus, maximizing $\mathcal{P}(\mathcal{L}(\tilde{H}_{1,2}^i) \in [\xi_q, \xi_{q+1}])$ leads to the lowest BMR and the optimal $\xi_q^\star$. In particular, classical encoding techniques, e.g., gray coding or XOR coding, can be employed to generate secret key for data encryption/decryption, based on the $\mathcal{L}(\tilde{H}_{1,2}^i)$. As shown in Fig. 1, from t_{D1} to t_{Dn-1}, the encrypted data is disseminated from the source node to the sink, while the receiver replies ACK to the sender at each hop.

III. Testbed and Experiments

We implement the cooperative secret key generation on a 2-hop WSN testbed, as shown in Fig. 2. Specifically, the source node, i.e., node 1, disseminates data packets to node 3 via node 2. Data packet rate is fixed at 1 packet/s. We conduct an experiment with different inter-node distance to evaluate the security protocol in terms of BMR. In particular, BMR is defined as the number of bits that do not match between the source node and the sink node divided by the number of bits extracted from RSS quantization.

Fig. 3 shows preliminary experimental results of BMR given $Q = 2$, $Q = 3$, or $Q = 5$. In general, increasing the inter-node distance leads to an increase of secret bit mismatch, since the low RSS causes a high randomness of $H_{i,j}$, which downgrades $\mathcal{P}(\mathcal{L}(\tilde{H}_{1,2}^i)$. Moreover, as the total number of quantization intervals increases from 2 to 5, the BMR goes up. When the inter-node distance is $10m$, BMR of the protocol with $Q = 5$ is 12%, which is 4.8% higher than the one with $Q = 2$. Therefore, it can be known that a smaller Q reduces $\mathcal{P}(\mathcal{L}(\tilde{H}_{1,2}^i)$. However, we also note that a smaller Q leads to a lower randomness of the secret key, which is easier to be cracked by the eavesdropper.

IV. Future Work

Based on the experiments on the 2-hop WSN testbed discussed in the previous section, we observe that the distance between the nodes and number of quantization intervals affect the secret bit mismatch rate, hence the importance of dynamically tuning the quantization window. For future work, the WSN testbed will be extended to a large scale, and the proposed security protocol will be further evaluated in different applications of CPS, e.g., automotive scenarios and smart cities.

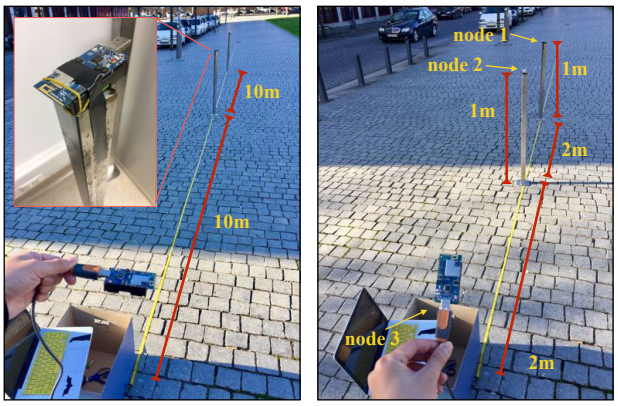

Fig. 2: The 2-hop WSN testbed.

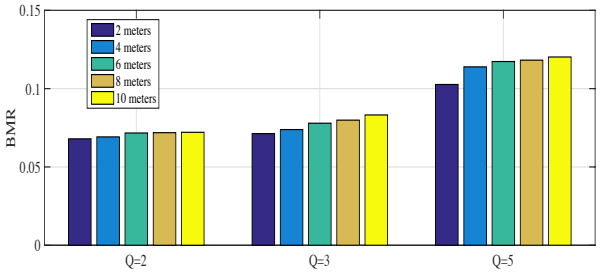

Fig. 3: BMR for varying inter-node distance.

Acknowledgement

This work was partially supported by National Funds through FCT (Portuguese Foundation for Science and Technology) within the CISTER Research Unit (CEC/04234); also by FCT and the EU ECSEL JU under the H2020 Framework Programme, within project ECSEL/0002/2015, JU grant nr. 692529-2 (SAFECOP).

References

[1] K. Li, W. Ni, E. Tovar, and M. Guizani, "LCD: Low latency command dissemination for a platoon of vehicles," in *IEEE International Conference on Communications (ICC)*. arXiv preprint arXiv:1801.06153, 2018, to appear.

[2] I. Stojmenovic, "Machine-to-machine communications with in-network data aggregation, processing, and actuation for large-scale cyber-physical systems," *IEEE Internet of Things Journal*, vol. 1, no. 2, pp. 122–128, 2014.

[3] C. Lu, A. Saifullah, B. Li, M. Sha, H. Gonzalez, D. Gunatilaka, C. Wu, L. Nie, and Y. Chen, "Real-time wireless sensor-actuator networks for industrial cyber-physical systems," *Proceedings of the IEEE*, vol. 104, no. 5, pp. 1013–1024, 2016.

[4] D. Trihinas, G. Pallis, and M. D. Dikaiakos, "ADMin: Adaptive monitoring dissemination for the internet of things," in *INFOCOM*. IEEE, 2017, pp. 1–9.

[5] K. Zeng, "Physical layer key generation in wireless networks: challenges and opportunities," *IEEE Communications Magazine*, vol. 53, no. 6, pp. 33–39, 2015.