DOI 10.5162/iCCC2024/1.2

Security Mean Distribution in WSNs for Cooperative Schemes

Benjamin Förster[1], *Thomas Hinze*[2] *and Peter Langendörfer*[1]
[1] Leibniz Institute for High Performance Microelectronics (IHP), 15236 Frankfurt (Oder), Germany
[2] Friedrich Schiller University Jena, 07743 Jena, Germany
bfoerster@ihp-microelectronics.com

Summary: Large-scale static wireless sensor networks (WSNs) are severely constraint in terms of energy resources and computation power while expected to provide their services for many years, guaranteeing a certain degree of requirement-based security. We propose a variation-based partitioning scheme for security mean distributions in favour of requirement-based cooperative security schemes for WSNs. We discuss advantages, applications and evaluate their computability and result quality on varying network sizes.

Keywords: wireless sensor networks, cooperation, collaboration, security, partitioning, distribution

Introduction

WSNs face inherent constraints such as limited energy supply and computing power, necessitating a delicate balance between network security and resource utilization. This becomes particularly critical in scenarios involving large-scale static WSNs with a limited number of base stations (BSs), where the security of data is pivotal for an informed decision process. Additionally, such networks are required to handle potential threats in between nodes without consulting a BS to ensure a timely reaction. To address these challenges, we propose a partitioning scheme that determines the distribution of security means by minimising the variance of the number of security mean types in each node's neighbourhood. Our scheme prioritises proximity in the allocation of security resources, enabling a *security-as-a-service* (SecAAS) approach akin to a neighbourhood watch, fostering mutual protection among nodes. SecAAS as used in this publication incorporates multiple cooperative and collaborative interrelations of security means in between nodes of a WSN. An optimal distribution of cooperative security means reduces the communication costs and allows adaptive load balancing (LB). The uniform distribution of security means ensures the availability of multiple occurrences of each type in proximity of every node, allowing for dynamic associations and capacity utilisations. For instance, this can involve dynamically adjusting service frequency or the number of nodes involved in cooperation as needed. Therefore, the proposed partitioning scheme limits the degrees of freedom by offering a general purpose solution for the distributing cooperating security means within WSNs.

To achieve this, we propose a partitioning scheme determining the minimal sum of variances of the number of security mean types in each node's h-hop neighbourhood for a given WSN topology. A partitioning divides the network into a fix number of sets, each representing a security mean type. The h-hop neighbourhood of a node v in a graph is defined as the set of nodes reachable from v traversing at most h edges. The partitioning scheme is computed using mixed integer quadratic programming (MIQP) and approximated using mixed integer linear programming (MILP). The MIQP minimises the sum of all variances resulting from each node's h-hop neighbourhood. The MILP approximates the variance by minimising the sum of the differences of the largest and smallest number of occurrences of security mean types in each node's h-hop neighbourhood. Determining the partitions using MIQP and MILP represents NP-hard problems. All graphs considered throughout this publication are undirected.

Related Works

Several established ensemble security frameworks [1, 2, 3] integrate varied security means to address specific use-cases and security needs tailored for specially designed WSNs. Ensemble refers to the integration of multiple different security means, extending beyond the scope and limitations of multi-layer concepts, for example. They offer effective and thorough security solutions considering the constraints imposed by WSNs. However, their specialisation severely restricts the area of application and therefore limits those security solutions to a few specific situations. This implicates that there is significantly limited potential for reusing or adapting the solution for varying problems and application areas.

Attempts to establish DSEs to determine requirement-based security configurations for WSNs [4, 5] and different cyber-physical systems in general [6, 7, 8, 9] address the shortcomings of specialised frameworks. Yet, existing solutions often neglect the consideration of complex ensemble security solutions with in-network interactions and complex communication patterns. Primarily to ensure that the resulting optimisation problems are manageable and to address the complexity involved in modelling the design space and associating its elements with required metrics [10]. There have been advancements in handling similarly complex DSEs [8, 9]. While a tailored security framework caters to specific needs with defined properties and network structures, allowing customised security mean distributions, a configuration designed to meet diverse requirements through automatic selection and blending of security means necessitates favourable security distribution/partitioning schemes. This predetermined setup reduces the complexity and increases the computability of resulting DSEs by restricting the number of variables (degrees of freedom) within the resulting exploration of the design space. In [11], we propose a partitioning scheme based on domatic partitions. It attempts to partition a graph in n disjoint sets so that there is a minimal number of empty intersections for all nodes in a graph with respect to the set of each node's neighbours and the sets of the partition. The partitioning scheme provides good solutions for situations, where the considered number of neighbours, resulting from the average node degree and chosen h-hop distance $|N[v]\backslash\{v\}|$, is lower or equal to the partition size n with $|\cdot|$ the set cardinality. In deviating cases, the remaining nodes will not contribute to the objective value and therefore are assigned randomly to any set of the partition. For those cases, we propose our variance- and spread-based partitioning schemes.

Partitioning Schemes and MIQP/MILP

Partitioning a graph representing a WSN into n sets by minimising the variance of the number of members within each node's neighbourhood ensures a balanced distribution of cooperating security means and therefore short pathways for in-network interactions, which in turn promotes better coordination among nodes. In a security framework tailored for specific security needs, characterised by precisely defined properties and a known network structure, the security mean distributions can be customised accordingly. However, in a configuration geared towards meeting diverse requirements by automatically selecting security means from a pool and blending them together based on given requirements, a predefined generally favourable security distribution becomes essential. This predefined distribution acts as a constraint, limiting the degrees of freedom in the resulting DSE.

The h-hop neighbourhood of a node $v \in V$ in a graph $G(V,E)$ is defined as the set of nodes reachable from v traversing at most h edges. In Equation (1), $x(v,i)$ are binary variables describing whether the node v is a member of set i ($x(v,i) = 1$) of a partition. The MIQP minimises the sum of the variance of n security mean types distributed in the inclusive neighbourhood $N[v]$ of each node $v \in V$ to determine a partition of size n:

$$\begin{aligned} \min\ & \textstyle\sum_{v\in V}\sum_{i=1}^{n}\left(\frac{|N[v]|}{n} - \sum_{w\in N[v]} x(w,i)\right)^2 \\ \text{s.t.}\ & \forall v \in V: \qquad \textstyle\sum_{i=1}^{n} x(v,i) = k \\ & \forall v \in V,\ \forall i \in [1,n] : x(v,i) \in \{0,1\} \end{aligned} \tag{1}$$

The h-hop inclusive neighbourhood of a node v refers to nodes reachable from v while traversing at most h edges, including v itself. The equality constraint ensures that each node is associated with precisely $k \in \mathbb{N}_{>1}$ security means. In our evaluation, we consider solely the case of $k = 1$ implying one security mean per node.

The MILP minimises the sum of the spread of n security mean types distributed on the inclusive neighbourhood $N[v]$ of each node $v \in V$ to determine a partition of size n:

$$\begin{aligned} \min\ & \textstyle\sum_{v\in V}(y_h(v) - y_l(v)) \\ \text{s.t.}\ & \forall v \in V: \qquad \textstyle\sum_{i=1}^{n} x(v,i) = k \\ & \forall v \in V,\ \forall i \in [1,n] : y_l(v) \le \textstyle\sum_{w\in N[v]} x(w,i) \\ & \forall v \in V,\ \forall i \in [1,n] : y_h(v) \ge \textstyle\sum_{w\in N[v]} x(w,i) \\ & \forall v \in V,\ \forall i \in [1,n] : x(v,i) \in \{0,1\}, \\ & \qquad y_l(v), y_h(v) \in \mathbb{N}_0 \end{aligned} \tag{2}$$

In every node's neighbourhood $N[v]$, $y_l(v)$ indicates the minimum occurrences of a specific security mean type, while $y_h(v)$ indicates the maximum number of occurrences. Each node's spread is the difference between its respective $y_h(v)$ and $y_l(v)$. Therefore, we minimise the sum of each node's spread.

Evaluation

To evaluate the computability of proposed partitioning schemes, we rely on our λ-precision UDG generator [11], creating graphs with average degrees of 4, 5 and 6 and node numbers of 20 to 300 in steps of 20 as specified in [11, Table 1]. For each of those parameter combinations, we generate 20 graphs. We evaluate the proposed partitioning schemes using Python, Pyomo and Gurobi by computing partitions of size 4 and 5 implementing the MIQP (1) and MILP (2). For the evaluation, we set the parameter $k = 1$ accordingly, constraining the partitioning schemes to one security mean per sensor node. Further, we set $h = 1$ for the hop-distance of each node's neighbourhood. For every partitioning, we present the outcome attained after a computation duration of 1200 seconds. After 1200 seconds, the computation stops, even if optimality has not been achieved.

For the comparison, we take for each graph $G(V,E)$ the mean of the variance of each node's neighbourhood $N[v]$ according to each node's association to a set of the partition $\overline{\sigma^2}(G) = \frac{1}{|V|}\sum_{v\in V}\overline{\sigma^2(\{I\cap N[v]\,|\,\forall I \in P\})}$ with P the partition of V containing n disjoint sets. Next, we compute the mean of these variances for each graph created with the same parameter set $\overline{\overline{\sigma^2}(G)}$. Our results confirm our prior assumption that the partitioning schemes from (1) and (2) significantly increase the uniformity of the security mean distribution for cases in which the partition size is smaller than the average node degree compared to optimal n-soft domatic partitions [11]. Optimality within the given time frame was less likely achieved for larger $|N[v]| - n > 0$. As example, take graphs with average node degree of 4, 1-hop neighbourhood and $n = 4$, of which all MIQPs from (1) have been computable to optimality for up to 180 nodes and for higher node numbers at least some graphs per sample set reached optimality. While for graphs with $|N[v] \backslash \{v\}| = 4$, 1-hop neighbourhood and $n = 3$, the optimality within the given time frame for the MIQPs from (1) was only achievable for all graphs per sample set of up to 60 nodes and for some graphs per sample set of up to 120 nodes. The pattern is consistent throughout all measurements. Further, while the mean of variance $\overline{\overline{\sigma^2}(G)}$ for smaller $|N[v]| - n > 0$ only slightly improves compared to the optimal n-soft domatic partitions, it significantly improves with the increasing difference $|N[v]| - n > 0$ even for non-optimal results. Estimating the variance partitioning concept (1) through the calculation of the spread (2) has demonstrated the same result quality as the variance for optimal results and only minimal inferior result quality for non-optimal results. The spread partitioning method achieves optimality in almost all cases compared to (1), it is surpassed by the optimal n-soft domatic partitioning scheme [11], which attains optimality across all tested scenarios. The $\overline{\overline{\sigma^2}(G)}$ is significantly worse for all solutions of the optimal n-soft domatic partition.

Conclusion and Applications

In this publication, we proposed two partitioning schemes allowing for generically applicable graph partitionings in favour of requirement-based security configurations combining arbitrary security means on WSNs. We have shown the computability and advantages of the proposed partitioning schemes over prior proposed optimal n-soft domatic partitions. Further, we have been able to illustrate the result quality of the proposed MIQP even in cases of non-optimality. The performance of the MILP approximating the variance using the spread (2) has proven to provide almost the same result quality as the variance with a significantly better computation time to optimality, which is reached in almost all test cases. While the optimal n-soft domatic partitioning [11] is still faster to compute, it does not compare with the variance per node results expressed by $\overline{\overline{\sigma^2}(G)}$.

There are a multitude of applications for the proposed partitioning scheme for large-scale static WSNs. Advantages of a partitioning for WSNs allowing a uniform distribution of security means are that the communication overhead of in-network interaction is reduced, the availability of multiple security means in local proximity of each node allows the efficient implementation of LB strategies, ensemble intrusion detection concepts, the application of secure comparative analysis strategies and secure aggregation strategies as well as combinations of those. It lowers communication overhead during in-network interactions, ensures the availability of multiple security means of the same type to handle failure-related topology changes, facilitating efficient implementation of LB strategies and ensemble-based intrusion detection concepts. Additionally, it supports the application of secure comparative analysis and secure aggregation strategies if sets of nodes of a partition implement encryption, message authentication codes, watermarking or information hiding strategies. These terms emphasise the secure assessment or evaluation of data integrity and authenticity between protected and unprotected sources within the network.

Ensemble security frameworks tailored to predefined WSNs with predetermined characteristics and specific security needs, including fixed sizes, known topologies, and well-defined partitioning, may yield superior outcomes in those particular scenarios. In contrast, our partitioning approach offers flexible solutions that can be configured to accommodate a wide range of use cases and diverse requirements. Moreover, it streamlines complex DSEs necessary for an automated requirement-based security configuration integrating collaborating security means.

Further concepts to consider and evaluate are combinations of optimal n-soft domatic partitions and variance/spread-based partitioning schemes. By integrating their objectives in a single optimisation problem, depending on its computability, we expect to attain synergistic advantages.

References

[1] W. Li, W. Meng, and L. F. Kwok, “Surveying trust-based collaborative intrusion detection: state-of-the-art, challenges and future directions,” *IEEE Communications Surveys & Tutorials*, vol. 24, no. 1, pp. 280–305, 2021.

[2] M. Valero, S. S. Jung, A. S. Uluagac, Y. Li, and R. Beyah, *Di-sec: A distributed security framework for heterogeneous wireless sensor networks*. IEEE, 2012.

[3] H. Saxena, C. Ai, M. Valero, Y. Li, and R. Beyah, “Dsf-a distributed security framework for heterogeneous wireless sensor networks,” in *2010-MILCOM 2010 Military Communications Conference*, pp. 1836–1843, IEEE, 2010.

[4] V. Cionca, T. Newe, and V. T. Dădârlat, “Configuration tool for a wireless sensor network integrated security framework,” *Journal of Network and Systems Management*, vol. 20, pp. 417–452, 2012.

[5] S. Peter and P. Langendörfer, “Tool-supported methodology for component-based design of

wireless sensor network applications," in *2012 IEEE 36th Annual Computer Software and Applications Conference Workshops*, pp. 526–531, IEEE, 2012.

[6] N. Tsiskaridze, M. Strange, M. Mann, K. Sreedhar, Q. Liu, M. Horowitz, and C. W. Barrett, "Automating system configuration.," in *FMCAD*, pp. 102–111, 2021.

[7] P. Nuzzo, N. Bajaj, M. Masin, D. Kirov, R. Passerone, and A. L. Sangiovanni-Vincentelli, "Optimized selection of reliable and cost-effective safety-critical system architectures," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 39, no. 10, pp. 2109–2123, 2019.

[8] D. Kirov, P. Nuzzo, R. Passerone, and A. Sangiovanni-Vincentelli, "Optimized selection of wireless network topologies and components via efficient pruning of feasible paths," in *Proceedings of the 55th Annual Design Automation Conference*, pp. 1–6, 2018.

[9] D. Kirov, P. Nuzzo, R. Passerone, and A. Sangiovanni-Vincentelli, "Archex: An extensible framework for the exploration of cyber-physical system architectures," in *Proceedings of the 54th Annual Design Automation Conference 2017*, pp. 1–6, 2017.

[10] A. Ramos, B. Aquino, M. Lazar, R. Holanda Filho, and J. J. Rodrigues, "A quantitative model for dynamic security analysis of wireless sensor networks," in *GLOBECOM 2017-2017 IEEE Global Communications Conference*, pp. 1–6, IEEE, 2017.

[11] B. Förster, P. Langendörfer, and T. Hinze, "Determining distributions of security means for wireless sensor networks based on the model of a neighbourhood watch," *arXiv preprint arXiv:2212.09050*, 2022.