

WISE: Lightweight Intelligent Swarm Attestation Scheme for IoT (The Verifier's Perspective)

Mahmoud Ammar
imec-DistriNet, KU Leuven
mahmoud.ammar@cs.kuleuven.be

Mahdi Washha
IRIT, Toulouse University
mahdi.washha@irit.fr

Bruno Crispo
imec-DistriNet, KU Leuven
Trento University, Italy
bruno.crispo@unitn.it

Abstract—The growing pervasiveness of Internet of Things (IoT) expands the attack surface by connecting more and more attractive attack targets, i.e. embedded devices, to the Internet. One key component in securing these devices is software integrity checking, which typically attained with *Remote Attestation* (RA). RA is realized as an interactive protocol, whereby a trusted party, *verifier*, verifies the software integrity of a potentially compromised remote device, *prover*. In the vast majority of IoT applications, smart devices operate in swarms, thus triggering the need for efficient swarm attestation schemes.

In this paper, we present WISE, the first intelligent swarm attestation protocol that aims to minimize the communication overhead while preserving an adequate level of security. WISE depends on a resource-efficient smart broadcast authentication scheme where devices are organized in fine-grained multi-clusters, and whenever needed, the most likely compromised devices are attested. The candidate devices are selected intelligently taking into account the attestation history and the diverse characteristics (and constraints) of each device in the swarm. We show that WISE is very suitable for resource-constrained embedded devices, highly efficient and scalable in heterogeneous IoT networks, and offers an adjustable level of security.

Index Terms—Internet of Things (IoT), security, remote attestation, swarm, scalability, online learning, malware detection.

I. INTRODUCTION

Nowadays, Internet-connected embedded devices are increasingly deployed in many aspects of modern life. Unfortunately, such devices represent attractive targets for cyber attacks as they are used in a wide range of applications where they process privacy-sensitive information and perform safety-critical tasks. Furthermore, the specialized nature of these devices in terms of limited resources and computing power hinders the realization of strong security mechanisms to prevent cyber attacks. Hence, attacking such devices would result in very severe consequences, exemplified by Stuxnet [1].

Remote attestation (RA) is a well-known security service that enables the detection of malware-infected devices. It allows a trusted entity, denoted as a *Verifier*, to verify the internal state of remote untrusted IoT device, denoted as a *Prover*, by measuring its software integrity. Traditional attestation protocols [2]–[4] consider only a single prover device. However, the diverse applications of IoT are naturally distributed and often embedded in numerous heterogeneous computing devices deployed over wide geographical areas, forming self-organizing mesh networks or swarms. Therefore, applying traditional attestation protocols in such scenarios is

inefficient and entails a significant overhead, as the verifier has to run the attestation protocol with each device individually.

Problem Statement. Recently, a number of research proposals have been introduced to address swarm attestation [5]–[11]. To this end, all of these attestation schemes are efficient and reduce the communication overhead compared to the naive approach of applying many times single prover attestation. Nevertheless, they are still rigid and not smart enough to adapt the different requirements of the various IoT devices, as whenever attestation takes place, all devices in the swarm are involved without any distinction. However, in real scenarios, connected devices in a mesh network have different software configurations and possess heterogeneous hardware capabilities. Therefore, the *equality* approach followed by existing attestation schemes still incurs substantial overheads. First, it is harmful to engage safety-critical and time-sensitive devices in periodic and potentially expensive (in terms of time and energy) RA, especially when the attestation history shows that they have never been compromised or rarely so. Second, efficiency as a feature of scalable attestation is maintained through many factors, and one of them is the aggregation of attestation reports to reduce the message size. Larger the network, the bigger is the size of the aggregate. Many IoT devices (such as IETF Class-1 [12]) have very limited memories that are not sufficient enough to authenticate and store a big-sized aggregate before propagating it till reaching the verifier. Third, the vast majority of available attestation schemes assume time synchronization which is difficult to handle in heterogeneous environments and incurs an extra overhead. Last, the nature of some devices (due to their locations, time-sensitivity, tasks, being previously compromised, etc.) requires to be more frequently attested than others and vice versa.

Contribution. We present WISE, a lightweight, intelligent, and scalable attestation protocol that is very suitable for static heterogeneous IoT networks, aiming for minimizing the communication overhead and thus power consumption. In WISE, the attestation of the entire swarm is distributed over a large time window, where a subset of devices is attested every time interval. The time window can be variable for each device or subset of devices as it is adjusted dynamically at the verifier side. WISE is smart in the sense that the verifier outputs a candidate subset of devices to be attested after performing online learning from the history of previous attestation periods

depending on Hidden Markov Model (HMM) [13], and taking into account the various individual needs and characteristics of connected devices in the swarm as conditions (or features).

Paper outline. The remainder of this paper is organized as follows. § II reviews the related work. A system model is presented in § III. § IV describes WISE in details, whereas § V highlights on the analytical model of the intelligence part of WISE. The security analysis of WISE is discussed in § VI. Implementation details and evaluations are reported in § VII. § VIII concludes the study.

II. RELATED WORK

Single Device Attestation. Prior work in single-prover RA can be divided into three main categories: hardware-based techniques [2] that rely on a built-in secure hardware (e.g. Trusted Platform Module (TPM)) in the prover device, software-based techniques [3] that do not require any hardware and depend only on some strict assumptions (e.g. accurate time measurements), and hybrid approaches [4] that build atop minimal hardware modifications to the existing low-end IoT platforms [14]. Abstractly speaking, each of these categories has pros and cons. Nevertheless, all of them target a single-device attestation. Accordingly, they are not efficient for swarm attestation.

Swarm Attestation. The recently proposed attestation schemes [5]–[11], [15] have addressed the attestation problem at a large scale where a significant number of devices have to be attested efficiently and securely. These proposals differ from each other in various ways: (i) the attestation protocol implemented (e.g. interactive [5]–[8], [10], [11], [15] or non-interactive [9]), (ii) the methodology followed in attesting the entire swarm (e.g. tree-based approaches [5]–[10], [15] or distributed ones [11]), (iii) the adversary model considered (e.g. remote-only attacker [5], [6], [8], [9], or remote and physical attackers [7], [10], [11], [15]), (iv) the type of the mesh network (e.g. highly dynamic one [11], or fairly dynamic and static topology [5]–[10], [15]), (v) the consideration of the mesh network (e.g. neighbour discovery, heterogeneity, broadcasting, unicasting, etc.), and (vi) the cryptography employed (symmetric key [8], [10], [15], public key [6], [11], or both [5], [7]).

To the best of our knowledge, all existing swarm attestation protocols attest all devices in the swarm whenever the attestation routine is conducted. Hence, we propose WISE, a smart and flexible swarm attestation protocol.

III. SYSTEM MODEL

Overview. We consider a mesh network with various heterogeneous low-end embedded devices. The network should be static or quasi-static¹ which we argue that this is the case of the majority of IoT application domains (e.g. smart buildings, etc.). The verifier should know in advance the exact network topology. Henceforth, we refer to the verifier as v and the prover as ρ .

¹Devices only move within the same covering communication range as when they are static.

Device Requirements. We assume that each device D_i in a swarm S satisfies the minimum hardware properties required for secure RA [14] which are ROM and memory protection unit (MPU). The ROM is needed to store the attestation routine and cryptographic keys, whereas the MPU is required to enforce access control over secret data. Also, we assume that v is a powerful device, i.e. Raspberry PI class or higher.

Adversary Model. We consider a software-only adversary, adv , who has the ability to perform remote attacks (Dolev-Yao model [16]). Thus, adv has full access to the network and can either perform passive (e.g. eavesdrop on communication, etc.) or active (e.g. inject a malware, etc.) attacks. In line with the majority of existing swarm attestation techniques, We rule out all kinds of DoS and physical attacks.

IV. WISE: PROTOCOL DESCRIPTION

Overview. WISE is a smart scalable attestation protocol which consists of two different phases. The first phase (§ IV-A) takes place once before the deployment where all devices are initialized by a trusted party (in our case, v) with some public and private data, and distributed logically over different clusters. In the second phase (§ IV-B), whenever needed, v performs the collective attestation over a subset of devices (instead of the entire swarm) that are wisely selected depending on the attestation history of every device and taking into account the individual characteristics of these devices.

A. Initialization Phase

v initializes each ρ with two device-specific keys for mutual authentication (dk_i) and attestation (ak_i) purposes, and one master key that is shared among all devices at the swarm-level (k_m). Also, each ρ stores its own unique ID (D_i), and the message authentication code (MAC) of the correct software state (M_s) of its memory (MeM), computed using ak_i .

Based on the recent taxonomies of addressing security challenges and IoT attacks [17], [18], we identify five main categories to classify IoT devices, where each category has different clusters and every cluster has a unique ID (c_i):

- Geographical Location: ρ 's are divided into clusters based on their geographical locations.
- Software Configurations: ρ 's are grouped into clusters according to partial or full similarities in their software.
- Hardware Capabilities: ρ 's are grouped into clusters according to the type of hardware they possess.
- Security & Safety: its an application-dependent feature which classifies ρ 's according to how critical they are to

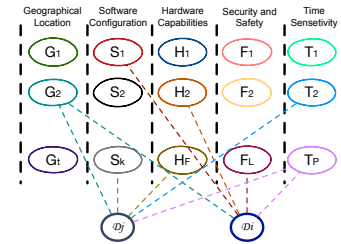


Fig. 1: An example of classifying two devices into clusters

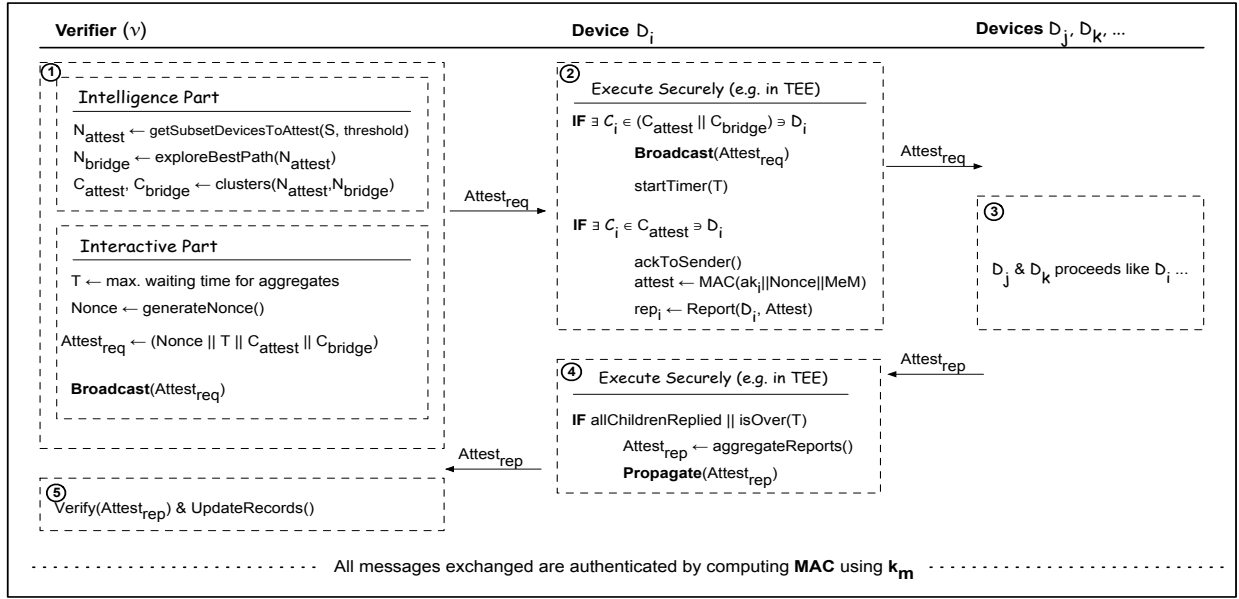


Fig. 2: An overview of the attestation phase in WISE

the application domain considering a combination of the task they perform and the security mechanism employed by the hosting hardware.

- Time Sensitivity: ρ 's are classified into clusters according to their time constraints and how critical is it to deviate them frequently from doing their tasks.

Number of clusters in each category is an application-dependent value. Each ρ should *virtually* belong to one cluster of each category by storing its identifier (c_i) in its memory as shown in Figure 1. The goal of the multi-clustering technique is twofold; First, it reduces the communication overhead in terms of number and sizes of exchanged packets, as explained in § V. Second, over time, v can learn from the attestation history the behavior of adv by realizing the clusters that have frequently compromised devices, thus being able to patch common vulnerabilities. Please note that the selection criteria of categories and clusters is flexible as more or less categories can be considered depending on the application domain.

B. Attestation Phase

Initially, v initiates the attestation routine for all devices as there is still no history and thus all ρ 's in the swarm are attested. Depending on authenticated broadcast messages, v propagates an attestation request ($Attest_{req}$), containing a *nonce* to avoid replay attacks, to all ρ 's in the vicinity, which is then further propagated in the network via broadcasting too, thus forming a virtual spanning tree. $Attest_{req}$ contains also the maximum time (T), through which, each ρ has to send a valid reply, where T is adjusted w.r.t the slowest ρ included in that attestation. The calculation of various time values takes place once all classes of devices are in a healthy state at deployment time to avoid delay-related attacks (e.g. downgrade or black hole attacks) [19]. Therefore, every receiver ρ acknowledges receiving $Attest_{req}$ to the sender device, thus determining the number of replies that should be received.

Each ρ answers $Attest_{req}$ by producing an attestation report (rep_i). rep_i consists of the device identifier (D_i) in addition to an attest value reflecting its state. All attestation reports are propagated back after being aggregated at every intermediate ρ using a secure aggregation scheme [20] till reaching v .

After running the attestation routine few times ², v starts behaving smartly by distributing the attestation over a dynamically variable time window, where each time the most likely compromised devices are only attested (see ① in Figure 2). In the selection process of the candidates, v takes into account the following factors: (i) the attestation history of each ρ and its direct neighbours, (ii) the ratio of compromised devices in every cluster that ρ belongs to, (iii) the maximum time that ρ could stay without being attested (this is specified in the initialization phase), (iv) the degree of importance of ρ 's task to be attested more often (this can be inferred from Security & Safety category), and (v) the time constraints of ρ w.r.t real time tasks that should not be interrupted (or rarely so). In principle, other criteria can be considered in the selection process of devices and the frequency of performing attestation. The minimum number of candidates (i.e. *threshold*) is an application-dependent value.

In order to keep the size of $Attest_{req}$ small, the attestation target will be at the cluster-level. Therefore, upon learning, v finds out the near-optimal set of clusters (C_{attest}) (in terms of number of devices and number of hops) that cover the output candidates in order to minimize the communication overhead (given the network topology). Furthermore, if some of the selected devices are not directly reachable by v or by other selected devices, v finds out the minimal set of clusters

²Number of times is an application-dependent value that determines the level of confidence. In our case, we consider the worst scenario when the attacker behaves randomly. Therefore, a high number of times, e.g. thousands of times, does not really enhance the accuracy. In the experiment section later on, we adjust this number to be only 100 times.

(C_{bridge}) that would participate in the attestation routine as bridges. Their goal is only broadcasting the received $Attest_{req}$ and then propagating the delivered attestation reports. Unless there are no other alternatives to reach some or all devices in C_{attest} , v avoids including the clusters that contain time-sensitive devices in C_{bridge} .

Once both sets of clusters are generated, v creates $Attest_{req}$ containing them along with the *nonce* value and T . Any receiver ρ re-broadcasts $Attest_{req}$ if it belongs to one of the clusters included in either sets, and computes its attestation report if it is only a member in one of the clusters in C_{attest} (see ②). Finally, each ρ propagates the aggregate of attestation reports if either all children are replied or the maximum waiting time is over (see ④). v verifies the delivered aggregates and accordingly updates the history records of each ρ , and then measures are taken against compromised devices, i.e. *secure erasure* [21].

V. WISE: ANALYTICAL MODEL

In this section, we describe the formal mathematical model of the intelligence part of WISE, whereas in the next section (§ VI), we analyze the security of our protocol.

A. Notations and Definitions

Let $G(S, L)$ be a graph of an IoT mesh network where S (the swarm) is a finite set of devices (nodes) represented as $S = \{D_1, D_2, \dots, D_n\}$, and L is the set of direct links between nodes. We define k uncorrelated categories as $Cats = \{C_1, C_2, \dots, C_k\}$ where C_\bullet represents the category name (i.e. geographical). Each C_\bullet contains a set of clusters, defined as $C_\bullet = \{c_{\bullet 1}, c_{\bullet 2}, \dots, c_{\bullet m}\}$ where m is the number of clusters. Each $D_i \in S$ should belong to only one $c_{\bullet i}$ in every C_\bullet . In nutshell, the following properties must be satisfied:

- 1) **Non-overlapping:** For each C_\bullet , $\bigcap_{1 \leq i \leq |C_\bullet|} c_{\bullet i} = \emptyset$.
- 2) **Network Coverage:** For each C_\bullet , $\bigcup_{1 \leq i \leq |C_\bullet|} c_{\bullet i} = S$.
- 3) **Uniformity:** $\forall D_\bullet \in S, \sum_{i=1}^k |\{D_\bullet\} \cap \bigcup_{1 \leq j \leq |C_i|} c_{ij}| = k$.

Given the network topology, each $D_i \in S$ is represented as a $\langle key, value \rangle$ map, where *key* is the unique D_i and *value* is an 8-tuple of metadata represented as follows: $\langle D_{clusters}, T_{max}, D_{history}, D_{attest, t}, T_{last}, D_{neighbors}, D_{paths}, D_{degree} \rangle$. Each attribute is defined as follows:

- $D_{clusters}$: the k clusters where D_i is a member in.
- $T_{max} \in \mathbb{Z}^+$: the maximum time (in minutes) that D_i can stay without attestation.
- $D_{history}$: the attestation history of D_i , represented as an ordered finite set $\{a_0, a_1, \dots, a_{t-1}\}$, where $a_\bullet \in \{0, 1, x\}$ as 0 means that D_i was compromised, 1 refers to a healthy state, and x means that D_i has not been attested in the considered iteration.
- $D_{attest, t} \in \{0, 1, x\}$: the predicted attestation response in the current iteration (t).
- $T_{last} \in \mathbb{Z}^+$: the last time (in minutes) that D_i has been attested.

- $D_{neighbors} \subset S$: the set of devices that are directly connected with D_i , represented as $D_{neighbors} = \{D_j | l_{ij} \in L, D_j \in S\}$ where l_{ij} is an undirected link.
- D_{paths} : an ordered set of the top m shortest paths that v can follow to reach D_i . Each path is represented as a set of devices from source (v) to destination (D_i).
- $D_{degree} \in [1, |C_k|]$: it represents the degree of sensitivity w.r.t real time tasks where 1 means extremely sensitive.

B. Problem Formalization

Given the $\langle key, value \rangle$ map of devices, the intelligence part of WISE (see ① in Figure 2) can be represented as multi-objective optimization problem.

1) *Candidates Selection*: v leverages the attestation history of each D_i as a heuristic information for computing the probability of being uncompromised in the next attestation iteration. Considering the calculated probabilities of devices along with their time constraints, the candidates selection problem is formalized as follows:

$$\begin{aligned} & \text{minimize}_{\alpha_1, \dots, \alpha_{|S|}} \sum_{j=1}^{|S|} \alpha_j * Pr(D_j.D_{attest, t} = 1 | O_t) \quad \text{s.t.} \quad \sum_{i=1}^{|S|} \frac{\alpha_i}{|S|} \geq Th_{cov}, \\ & Min\{(1 - \alpha_i) * (D_i.T_{last} + D_i.T_{max} - T_{current}) : 1 \leq i \leq |S|\} > 0 \end{aligned} \quad (1)$$

where $|S|$ is the number of devices in the swarm, $\alpha \in \{0, 1\}$ is a binary free variable at which the optimization step is performed for either excluding (0) or including (1) D_j in the attestation, $Pr(D_j.D_{attest, t} = 1 | O_t)$ represents the probability of the j^{th} device being uncompromised in the current attestation iteration (once the interactive part takes place) given O_t as a set of features (observations), $T_{current}$ is the time (in minutes) of running the interactive part of the current iteration. Th_{cov} is a constraint in the objective function which represents the minimum ratio of devices to be covered. The second constraint guarantees attesting all devices within the predefined time window. The output is a set of the most likely compromised devices that is formally defined as $N_{attest} = \{D_i : D_i \in S, \alpha_i = 1\}$.

2) *Best Route Exploration (gap bridging)*: WISE depends on an authenticated broadcast technique to emit $Attest_{req}$. Getting $Attest_{req}$ delivered to all candidates selected in § V-B1 should incur a minimal communication and runtime overhead. Therefore, a minimum number of devices should be involved in delivering $Attest_{req}$ to the candidates and then propagating their aggregated reports to v . Unless there are no other alternatives, time-sensitive devices should not be involved and deviated from doing their main tasks. The gap bridging problem is formalized as follows:

$$\begin{aligned} & \text{minimize}_{\beta_1, \dots, \beta_{|P_{comb}|}} \sum_{\langle P_1, \dots, P_{|N_{attest}|} \rangle_j \in P_{comb}} \beta_j * \sum_{D_\bullet \in U_{D_i}} D_\bullet.D_{degree} \\ & \text{s.t.} \quad \sum_{i=1}^{|P_{comb}|} \beta_i = 1 \end{aligned} \quad (2)$$

where $P_{comb} = \prod_{a=1}^{|N_{attest}|} D_a.D_{paths}$ is the Cartesian product of the set of paths of each candidate device, $|P_{comb}|$ is the cardinality (length) of path combinations set, $\langle P_1, \dots, P_{|N_{attest}|} \rangle_j$

is the j^{th} tuple element in P_{comb} which corresponds to best (shortest) paths combination among $|P_{comb}|$ different possibilities, $\beta_j \in \{0, 1\}$ is a binary free optimization variable for the j^{th} paths combination, and $U_{Di} = \bigcup_{i=1}^{|N_{attest}|} P_i$ represents a set of nodes resulted by unifying a combination of shortest paths associated with the j^{th} tuple $\langle P_1, \dots, P_{|N_{attest}|} \rangle_j$. The imposed constraint is to ensure the selection of a single combination of paths. The output is a set of nodes, defined as $N_{bridge} = \{D_\bullet : \langle P_1, \dots, P_{|N_{attest}|} \rangle_j \in P_{comb}, D_\bullet \in \bigcup_{i=1}^{|N_{attest}|} P_i, \beta_j = 1\}$.

3) *Clusters Selection*: adding the IDs of candidate devices (along with bridge devices) to $Attest_{req}$ hinders the scalability as the message size will be big. This also sharply increases the communication overhead as well as the processing time at ρ side. We overcome this limitation by targeting the cluster-level. In such case, $Attest_{req}$ will include the identifiers of the minimal set of clusters that cover the selected devices w.r.t. the communication overhead. This is formalized as follows:

$$\begin{aligned} & \text{minimize} \quad \sum_{j=1}^k \sum_{i=1}^{|C_j|} \gamma_{ji} * ComOverhead(c_{ji}) \quad \text{s.t.} \\ & \forall D_\bullet \in N_{attest} \cup N_{bridge} \quad \sum_{j=1}^k \sum_{i=1}^{|C_j|} \gamma_{ji} * |c_{ji} \cap \{D_\bullet\}| \geq 1 \end{aligned} \quad (3)$$

where k is the number of categories, $|C_j|$ is the number of clusters in the j^{th} category, c_{ji} represents the i^{th} cluster in the j^{th} category, $ComOverhead(\bullet)$ is a function that computes the communication overhead in terms of number of hops, $\gamma_{ji} \in \{0, 1\}$ is a binary free variable at which the optimization process is performed so that 1 value means that the cluster c_{ji} is selected. The constraint imposes selecting the most relevant clusters to the unified set of $N_{attest} \cup N_{bridge}$. The output is two sets of clusters represented as $C_{attest} = \{c_{ji} : c_{ji} \in C_j, j \in \{1, \dots, k\}, i \in \{1, \dots, |C_j|\}, \gamma_{ji} = 1, c_{ji} \cap N_{attest} \neq \emptyset\}$, and $C_{bridge} = \{c_{ji} : c_{ji} \in C_j, j \in \{1, \dots, k\}, i \in \{1, \dots, |C_j|\}, \gamma_{ji} = 1, c_{ji} \cap N_{attest} = \emptyset\}$ respectively.

C. Probabilistic Model ³

To compute the probability component, $Pr(D_\bullet, D_{attest,t} | O_t)$, in the candidates selection problem, we use HMM for two main reasons. First, it computes the probability distribution of discrete hidden (unknown) states (i.e. compromised or uncompromised) over sequences (time-series) of observations (i.e. number of compromised neighbours). Accordingly, it is suitable to deal with the worst case scenario when the attacker works randomly. Seconds, in spite of assuming a powerful verifier, it is compact and very fast to use, compared to other techniques (i.e.

³We identify three heuristic approaches as solvers to provide near-optimal solutions for each of the formalized optimization problems. Due to the limited space, we omit the description of these approaches. To get the pseudo code of these solvers (or even the complete source code of the intelligence part), please contact the first author.

Recurrent Neural Networks) which are very time-consuming (iterative-based) and require a very big memory to store the $\langle key, value \rangle$ map when considering large mesh networks.

HMM notations. At any iteration t , two hidden states are identified: compromised ($D_{attest,t} = 0$) and uncompromised ($D_{attest,t} = 1$). Considering the $\langle key, value \rangle$ map, a vector of observations \mathbf{O}_t is formed for each D_\bullet by selecting M random independent variables (features). Given a sequence of observations $\{\mathbf{O}_1, \dots, \mathbf{O}_t\}$, learning $D_{attest,t}$ requires computing the following HMM parameters $\theta = \{\pi, H, b_{0,f_1}, \dots, b_{0,f_M}, b_{1,f_1}, \dots, b_{1,f_M}\}$:

- The state transition matrix (H): it contains the probabilities of transitioning from a state to the other. For instance, $h_{0,1}$ is the probability of D_\bullet to be healthy given that D_\bullet 's previous state is compromised (i.e. $Pr(D_{attest,t} = 1 | D_{attest,t-1} = 0)$).
- The initial state probability distribution (π): it initializes the probability distribution over $|Q|$ values, where Q is the set of hidden states and $|Q|$ is its cardinality.
- The emission (observation) probability distributions ($\{b_{1,f_1}, \dots, b_{1,f_M}, b_{0,f_1}, \dots, b_{0,f_M}\}$): it requires $|Q| \times M$ distributions for inferring values. For instance, b_{0,f_1} is the probability distribution of observing the value of feature f_1 (i.e. number of compromised devices in a joint cluster) when D_\bullet is predicted to be compromised.

Probability Computation. By leveraging the D_\bullet 's attestation history set ($D_{history}$), we estimate the HMM parameters, θ , using the Maximum Likelihood Estimation (MLE) method for a given set of observations. More precisely, the MLE finds the values that maximize the likelihood of generating the given observations. This is formalized as:

$$\begin{aligned} \theta_{mle} = \arg \max_{\theta \in \Theta} Pr(L | \theta) \quad \text{s.t.} \quad & \sum_{i \in Q} \pi_i = 1, \\ & \prod_{j \in Q} \sum_{i \in Q} h_{i,j} = 1, \quad \prod_{i \in Q} \prod_{v \in \{1, \dots, M\}} \int_{\mathbb{R}} b_{i,v}(x) dx = 1 \end{aligned} \quad (4)$$

where Θ is the search space of HMM parameters, $L = \{(x_1, y_1), \dots, (x_m, y_m)\}$ is a set of m distinct groups of paired sets of observations and D_\bullet 's attestation responses, $(x_\bullet, y_\bullet) = (\{\mathbf{O}_{t_1}, \dots, \mathbf{O}_{t_2}\}, \{a_{t_1}, \dots, a_{t_2}\})$, $1 \leq t_1 < t_2$, x_\bullet is a sequence of observation (feature) vectors, and y_\bullet is a sequence of true hidden states from iteration t_1 to t_2 . The first two constraints should equal 1 according to the HMM. The last constraint is associated to $|Q| \times M$ emission probability distributions where the area under each distribution should equal 1 and accordingly the multiplication of the $|Q| \times M$ distributions area equals 1.

The probability of generating any sequence of observations can be written using the HMM parameters θ as follows:

$$\begin{aligned} Pr((x_\bullet, y_\bullet) | \theta) = & \prod_{i \in Q} \pi_i^{f(i, y_\bullet)} * \prod_{i \in Q} \prod_{j \in Q} h_{i,j}^{f(i, j, y_\bullet)} \\ & * \prod_{i \in Q} \prod_{\mathbf{O}_t \in x_\bullet} \prod_{o_t, v \in \mathbf{O}_t} b_{i,v}(o_t, v)^{f(i, v, o_t, v, x_\bullet, y_\bullet)} \end{aligned} \quad (5)$$

where $f(i, y_\bullet)$ is an integer $\in [0, 1]$ representing the occurrence of the state i given a sequence y_\bullet , $f(i, j, y_\bullet)$ is the

number of occurrences of having a transition from the state j to i in the given true states sequence y_\bullet , and $f(i, v, o_{t,v}, x_\bullet, y_\bullet)$ is the number of times of observing the value $o_{t,v}$ of feature v in the given sequence of observations x_\bullet and true hidden states y_\bullet when the HMM process is in the state i .

The values of θ parameters can be obtained by assuming that for each sequence of the training m groups, the probability of generating L equals to the probability multiplication of generating each sequence individually, formalized as:

$$Pr(L|\theta) = \prod_{l=1}^m Pr((x_l, y_l)|\theta) = \prod_{l=1}^m \left(\prod_{i \in Q} \pi_i^{f(i, y_\bullet)} \right) * \prod_{i \in Q} \prod_{j \in Q} h_{i,j}^{f(i, j, y_\bullet)} \prod_{i \in Q} \prod_{\mathbf{o}_t \in \mathbf{x}_\bullet} \prod_{o_{t,v} \in \mathbf{o}_t} b_{i,v}(o_{t,v})^{f(i, v, o_{t,v}, x_\bullet, y_\bullet)}$$

$Pr(L|\theta)$ is a concave function having only one global maximum value. Hence, we compute the partial derivatives of $Pr(L|\theta)$ w.r.t each free parameter in θ . Thus, the values of HMM parameters that make each of the partial derivatives equals to zero ($\frac{\partial Pr(L|\theta)}{\partial \pi_{1,1}} = 0$, $\frac{\partial Pr(L|\theta)}{\partial \pi_1} = 0$, $\frac{\partial Pr(L|\theta)}{\partial b_{0,f_1}} = 0$, ...) are computed as follows:

$$\pi_i = \frac{\sum_{l=1}^m f(i, y_l)}{\sum_{k \in Q} \sum_{l=1}^m f(k, y_l)} \quad h_{i,j} = \frac{\sum_{l=1}^m f(i, j, y_l)}{\sum_{k \in Q} \sum_{l=1}^m f(i, k, y_l)} \quad (7)$$

$$b_{i,v}(o) = \frac{\sum_{l=1}^m f(i, v, o, x_l, y_l)}{\sum_{l=1}^m \int_{\mathbb{R}} f(i, v, o', x_l, y_l) do'} \quad (8)$$

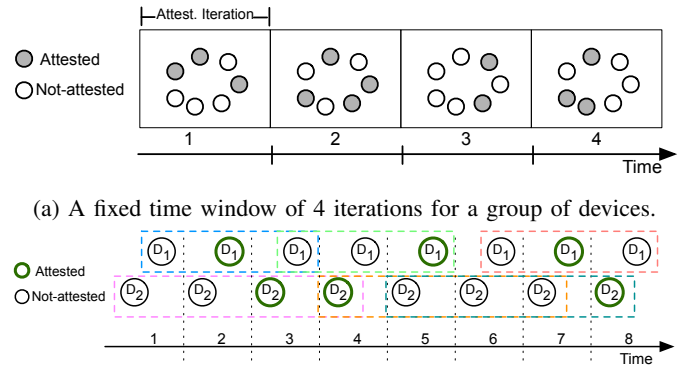
The resulted values are normalized and accordingly they implicitly satisfy the constraints in eq. (4).

Inference. Given the resulted HMM parameters, for any D_\bullet , the probability of being uncompromised at iteration t is computed as:

$$Pr(D_\bullet \cdot D_{attest,t} = 1 | \mathbf{O}_t) = \sum_{j \in Q} \pi_j h_{1,j} \prod_{o_v \in \mathbf{O}_t} b_{1,v}(o_v) \quad (9)$$

VI. WISE: SECURITY ANALYSIS

In principle, the time constraint in eq. (1), that is demonstrated by either a variable time window for each device or a fixed one for all, makes WISE (in spite of being operating in a smart probabilistic way that maintains a minimum communication overhead) at the same deterministic security level as other existing swarm attestation schemes. For instance, other schemes verify the integrity of the entire swarm each particular period of time (e.g. every 6 hours). During this period (the time between two successive attestation routines), the status of devices is unknown as some of them might be compromised and accordingly they will remain compromised till the next attestation routine is launched. In contrast, WISE distributes the attestation over this long time period (time window), thus minimizing the communication overhead, and speeding up the slow detection of some compromised devices that may result because of the long period of inactivity. Furthermore, WISE has two other main advantages. First, it addresses the individual differences and characteristic of devices (e.g. some



(b) An example of variable time window for two devices, where it is 3 for D_1 and 4 for D_2 .

(6) Fig. 3: An overview of the timing technique used in WISE that ensures covering all devices in the attestation within a variable/ fixed time window.

devices has to be more frequently attested than others and vice versa as shown in Figure 3 where both fixed and variable time window techniques are illustrated). Second, it is robust against a roving malware⁴, whereas all other existing schemes are not. In WISE, such kind of malware can not be aware of the attestation schedule because the time window of any device could be variable and represents only the upper bound, by which, the device should be attested at least once, whereas it could be many times as shown for some devices in Figure 3a, depending on the output of the intelligence mechanism employed. In nutshell, WISE allows to accommodate different risk levels, rather than adopting a single one as existing schemes, since for big mesh networks, it is unrealistic to assume that all nodes have the same level of exposure to attacks. A higher risk level requires more frequent attestation than a lower one.

In particular, the communication cost in WISE depends on the tolerated latency of detecting (possibly) compromised devices, where in each attestation iteration A_i , m out of n devices are attested, and m is an application-dependent value referring to the likelihood of a device to be compromised. WISE avoid starvation cases by identifying a (variable) maximum time window (W), through which, each D_i is attested at least once. We elaborate on the security of WISE in two streams: (i) per time window, and (ii) per attestation iteration.

A. Security of WISE per time window.

This is formalized by the following adversarial experiment $ATT_{adv}^{n,c}(j)$, where adv interacts with n devices, and compromises up to c devices in S according to the adversarial model presented in § III, where $0 \leq c \leq n$. Considering that adv is computationally bounded to the capabilities of the devices deployed in S , adv interacts with the devices a polynomial number of times j , where j is a security parameter. v verifies

⁴Roving malware is an advanced kind of malware that is always aware of the attestation schedule of the IoT device and thus it is only active between any two successive attestation routines which deletes itself at the beginning of the attestation to evade detection.

the attestation aggregates received in all A_i 's within the time window (W) and outputs a decision as 0 or 1. Denoting the decision made as A , $A = 1$ means that all devices are attested and compromised ones are detected, or $A = 0$ otherwise.

Theorem 1. *WISE is secure if $Pr[A = 1 \mid ATT_{adv}^{n,c}(j) == A]$ is negligible for $0 < c \leq n$.*

Proof. Considering eq. (1), $\forall D_\bullet \in S$:

$$\bigcup_{i=1}^W \{D_{attest,i}\} \cap \{0,1\} \neq \emptyset \quad (10)$$

In other words, each D_\bullet in S will be attested g times within W w.r.t T_{max} (see § V-A), where $1 \leq g \leq |A_i|$. It is important to mention that this is valid under the assumption that both MAC and aggregation schemes are secure and the attestation routine in the device itself is atomic. \square

B. Security of WISE per attestation iteration (A_i).

The security of WISE per A_i is a probabilistic value which range from $(1 - \frac{m}{n})$ to 1, where $(1 - \frac{m}{n})$ is the worst case when all unselected devices in the current attestation are compromised. Considering the probabilities calculated in eq. (9), we calculate the probability of having a secure swarm (no undetected compromised devices) as: $Pr[A_i = 1] \geq Th_{sec}$, where Th_{sec} is a security threshold computed as:

$$Th_{sec} = \frac{m}{n} + \frac{\sum_{D_\bullet \notin A_i} Pr(D_\bullet.D_{attest,t} = 1 | \mathbf{O}_t)}{n} \quad (11)$$

VII. IMPLEMENTATION & EVALUATION

A. Implementation

A prototype of WISE has been implemented over a heterogeneous mesh network consisting of 12 nodes with different hardware and software configurations where each node belongs to Raspberry PI, Arduino Uno, Arduino Due, Arduino Zero, Microship STK 600 with AVR Atmega644P MCU, or MicroPnP IoT platform [22]. Each platform is equipped with IEEE 802.15.4e radio transceiver for wireless communication. SHA-256 is employed as a keyed-hash message authentication code (HMAC) to measure the software integrity during the attestation phase. The precise time consumed by the various cryptographic and interactive operations in each platform is measured in order to simulate large mesh networks. A Raspberry PI 3 is selected to act as a verifier. In the implementation of HMM, the ratio of compromised neighbours along with the ratio of compromised devices in each corresponding cluster are selected as features (observations) for each device.

B. Evaluation

OMNeT++ framework [23] is used to simulate large networks with different configurations. The computational and network delays are adjusted according to the experimentally measured values in the prototype implemented. Three different scenarios are simulated, where each scenario composes of 10 different-sized networks ranging from 1k to 10k devices. The various mesh networks in all scenarios are deployed randomly. In scenario 1, the number of neighbours of each node is set

to be a random value from 1 to 5, whereas it is set to be from 1 to 7 in scenario 2 and from 2 to 10 in scenario 3.

Each contiguous group of devices are selected to be in the same geographical cluster with a fixed size of 30 (mostly), 20, or 10 devices. The devices are deployed randomly over other clusters in other categories. We assigned 6 different clusters in the hardware category and 30 clusters in the software one. The last two categories are composed of 10 different clusters each.

For each network in each scenario, we first run the attestation routine in a uniform state (all devices are attested) 100 times, where each time, we set up an adversarial model to attack randomly a number of devices ranging from 0 to 30% of the network size. After then, WISE takes place.

In all following figures, we set the minimum coverage of candidate devices per attestation iteration to be 20% of the network size, and the number of attacked devices is random in each iteration (0 to 30% of the network size).

Security and Robustness. Figure 4a and 4b represent two examples of two different-sized networks from scenario 1, where in each one, we show two cases of detecting high and low number of compromised devices. In these figures, the attack took place once before the first iteration. All compromised devices are detected by the 5th iteration (half of the longest time window as we modeled it as a variable discrete event in terms of number of iterations, where for each device, it is set to be a random value from 4 to 10).

Figure 4c shows the worst, average, and best ratio of detected compromised devices (per iteration) after running WISE 30 times in each of the thirty networks in all scenarios. Each time, a different number of devices is randomly compromised. The worst ratio was almost higher than 25%, whereas the average ratio was around 45% (with 20% coverage). Figure 4f shows the ratio of detected compromised devices if the attacker was targeting a specific class of devices (in our case, we modeled it to attack Arduino-zero cluster). Results show that the detection ratio with a targeted attacker is higher than the random one where in many iterations it was 100% at best, with an average of about 62%.

Scalability and Efficiency. Figure 4d and 4e illustrate the average size of aggregated reports and the number of exchanged messages in WISE respectively (compared to the traditional approach of attesting the entire swarm). Both figures show how efficient and scalable WISE is. We do not show the total runtime of WISE as it is hardware-dependent. Please note that WISE is always faster than other existing swarm attestation schemes as it only targets a subset of devices.

Memory footprint and Computation Time. At ρ side, WISE requires less than 100 bytes of permanent storage for storing the secret keys and clusters IDs, whereas it requires no more than 5 MB at v side to store a knowledge base ($< key, value >$ map) for a network consisting of 10k devices regardless the length of the attestation history. Computationally, for a network of 10k devices, the initial step that occurs once at v side (computing the shortest paths, etc.) requires no more than 6 minutes. Then, the intelligence part of WISE

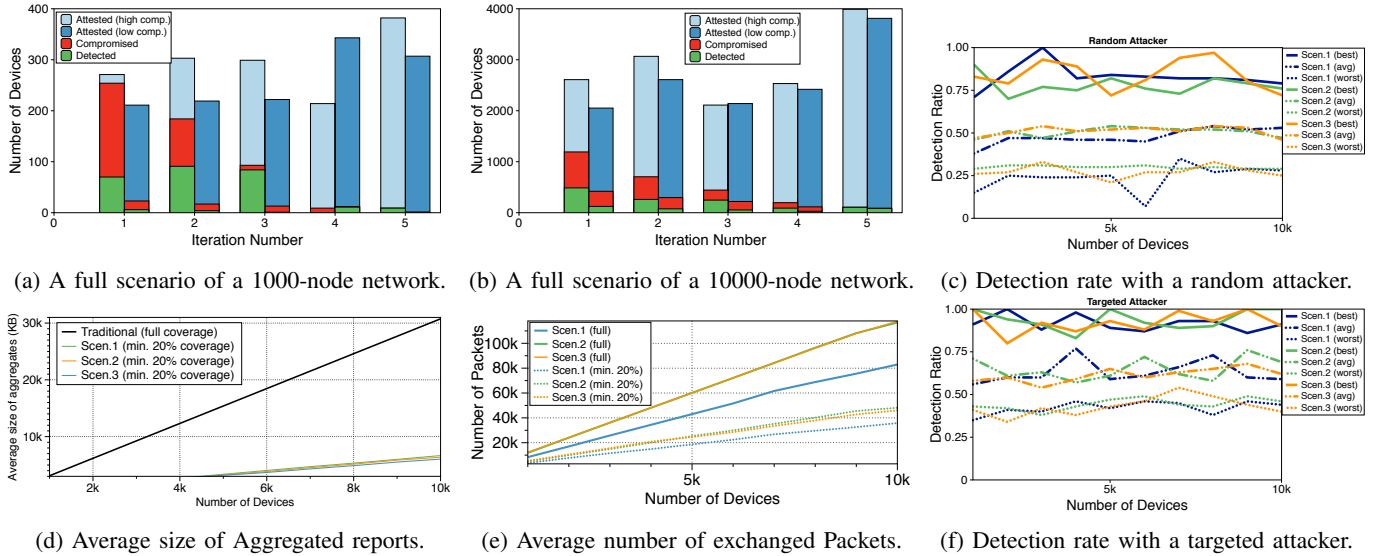


Fig. 4: An overview of diverse evaluation factors of WISE

requires less than 9 seconds each time. The verification of the attestation aggregates of 10K devices and updating the records in the knowledge base consumes no more than 3.5 seconds. The size of the attestation request did not exceed (at worst) 304 bytes for a network of 10k devices.

VIII. CONCLUSION

This paper presented WISE, the first smart swarm attestation protocol for the Internet of Things that relies on a resource-efficient machine learning technique using Hidden Markov Model. WISE is scalable and highly efficient to be used in (quasi-) static networks consisting of thousands of heterogeneous IoT devices. The minimized communication overhead depends on the tolerated latency of detecting (unlikely) compromised devices. This makes WISE very suitable to be used in various application domains, especially, in time-sensitive and safety-critical ones such as smart factories.

ACKNOWLEDGMENT

This research is supported by the research fund of KU Leuven and IMEC, a research institute founded by the Flemish government.

REFERENCES

- [1] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Security & Privacy*, vol. 9, no. 3, pp. 49–51, 2011.
- [2] B. Parno, J. M. McCune, and A. Perrig, "Bootstrapping trust in commodity computers," in *Security and privacy (SP)*, *IEEE symposium*, 2010.
- [3] Y. Li, J. M. McCune, and A. Perrig, "SBAP: Software-Based Attestation for Peripherals," in *Proceedings of the 3rd International Conference on Trust and Trustworthy Computing*, pp. 16–29, Springer-Verlag, 2010.
- [4] K. ElDefrawy, G. Tsudik, A. Francillon, and D. Perito, "SMART: Secure and Minimal Architecture for (Establishing Dynamic) Root of Trust," in *19th Annual NDSS Symposium*, The Internet Society, 2012.
- [5] N. Asokan, F. Brasser, A. Ibrahim, A.-R. Sadeghi, M. Schunter, G. Tsudik, and C. Wachsmann, "Seda: Scalable embedded device attestation," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, pp. 964–975, ACM, 2015.
- [6] M. Ambrosin, M. Conti, A. Ibrahim, G. Neven, A.-R. Sadeghi, and M. Schunter, "Sana: secure and scalable aggregate network attestation," in *Proceedings of the 2016 ACM CCS Conference*, pp. 731–742, 2016.
- [7] A. Ibrahim, A.-R. Sadeghi, G. Tsudik, and S. Zeitouni, "Darpa: Device attestation resilient to physical attacks," in *Proceedings of the 9th ACM WiSec Conference*, pp. 171–182, ACM, 2016.
- [8] X. Carpent, K. ElDefrawy, N. Rattanavipanon, and G. Tsudik, "Lightweight swarm attestation: a tale of two lisa-s," in *Proceedings of the 2017 AsiaCCS Conference*, pp. 86–100, ACM, 2017.
- [9] A. Ibrahim, A.-R. Sadeghi, and S. Zeitouni, "seed: secure non-interactive attestation for embedded devices," in *Proceedings of the 10th ACM WiSec Conference*, pp. 64–74, ACM, 2017.
- [10] F. Kohnhäuser, N. Büscher, S. Gabmeyer, and S. Katzenbeisser, "Scapi: a scalable attestation protocol to detect software and physical attacks," in *Proceedings of the 10th ACM WiSec Conference*, pp. 75–86, 2017.
- [11] F. Kohnhäuser, N. Büscher, and S. Katzenbeisser, "Salad: Secure and lightweight attestation of highly dynamic and disruptive networks," in *Proceedings of the 2018 AsiaCCS Conference*, ACM, 2018.
- [12] C. Bormann, M. Ersue, and A. Keranen, "Terminology for Constrained-Node Networks," RFC 7228, IETF, may 2014.
- [13] L. R. Rabiner, "A tutorial on hidden markov models and selected applications in speech recognition," *Proceedings of the IEEE*, vol. 77, no. 2, pp. 257–286, 1989.
- [14] A. Francillon, Q. Nguyen, K. B. Rasmussen, and G. Tsudik, "A minimalist approach to remote attestation," in *Design, Automation and Test in Europe Conference and Exhibition (DATE)*, IEEE, 2014.
- [15] M. Ammar, M. Washha, G. Sankar Ramachandran, and B. Crispo, "slimiot: Scalable lightweight attestation protocol for the internet of things," in *Proceedings of the 2018 IEEE Conference on Dependable and Secure Computing (DSC)*, IEEE, 2018.
- [16] I. Cervesato, "The dolev-yao intruder is the most powerful attacker," in *16th Annual Symposium on Logic in Computer Science—LICS*, 2001.
- [17] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in internet of things: The road ahead," *Computer networks*, vol. 76, pp. 146–164, 2015.
- [18] R. V. Steiner and E. Lupu, "Attestation in wireless sensor networks: A survey," *ACM Computing Surveys (CSUR)*, vol. 49, no. 3, p. 51, 2016.
- [19] P. Pongle and G. Chavan, "A survey: Attacks on rpl and 6lowpan in iot," in *Pervasive Computing (ICPC), 2015 International Conference on*, pp. 1–6, IEEE, 2015.
- [20] J. Katz and A. Y. Lindell, "Aggregate message authentication codes," in *Topics in Cryptology—CT-RSA 2008*, pp. 155–169, Springer, 2008.
- [21] M. Ammar, W. Daniels, B. Crispo, and D. Hughes, "Speed: Secure provable erasure for class-1 iot devices," in *Proceedings of the Eighth ACM Conference on Data and Application Security and Privacy*, pp. 111–118, ACM, 2018.
- [22] N. Matthys, F. Yang, W. Daniels, W. Joosen, and D. Hughes, "Demonstration of micropnp: the zero-configuration wireless sensing and actuation platform," in *SECON, 13th Annual IEEE Conference*, 2016.
- [23] A. Varga, "The omnet++ discrete event simulation system (<http://www.omnetpp.org>). european simulation multiconference, prague," 2001.