# Adaptive IoT Device Authentication Management Supported by Policies and Social Trust

**Yan Uehara**[*†], **Carlos Pedroso**[*†], **Michele Nogueira**[*†], **Aldri Santos**[*]
[*]Wireless and Advanced Networks Laboratory (NR2) - UFPR, Brazil
[†]Center for Computational Security sCience (CCSC) - UFPR, Brazil
Emails: {yumoraes, capjunior, michele, aldri}@inf.ufpr.br

***Abstract*—As the devices become present in different social and human settings they come in contact with sensitive information. In those situations, they need to verify other device's identities to interact with them. However, as multiple authentication mechanisms for IoT exists, systems capable to change the authentication mechanism in use becomes necessary. Adaptive authentication systems allow devices to react to modification in input factors and use a mechanism suitable to the situation they encounter. However, existing approaches do not consider the social relation that exists among devices as an adaptation factor. This paper introduces the GALENA system for adaptive authentication in IoT networks. It relies on social trust, derived from the device's social relations, as adaptation factor. Also, it employs policies to determine which the mechanism to use. Those techniques allows flexibility in the device authentication process and provides robustness in service relations.**

***Index Terms*—adaptive authentication, social trust, policies**

## I. Introduction

The interconnection of objects around us and the Internet caused the emergence of the Internet of Things (IoT). These computational devices creates an ubiquitous computational human and urban environment – like smart homes, intelligent transportation system, and smart healthcare – collaborating in several application domains, aiming to increase the quality of life of its inhabitants [1]. To achieve the goals of those domains IoT devices exchange messages and disseminate information over the network. Thus, these actions must take place in a safe manner given IoT devices' ubiquitous nature and their contact with our personal data. Security requirements, such as confidentiality, integrity and authentication, differ from one setting to another. Authentication, which is the verification of a device's attribute - commonly its identification, is identified as one of the key requirements of IoT [2] in order to prevent malicious devices from interfering with the network.

However, IoT devices usually suffer from processing, energy, and storage restrictions; They also establish a dynamic network due to their mobility. Thus, traditional authentication mechanisms have not been adapted to the IoT environment [3] and the restrictions and the need for secure communication have led to the emergence of multiple authentication mechanisms more suitable for IoT networks. Adaptive authentication systems change the authentication mechanism as the devices move across different domains [4]. They employ strategies to adapt, such as policies and machine learning. The policy strategy comprises the approaches normally applied to carry out self-adaptive management [5]. That strategy contributes to the adaptation process by mapping causes of adaptation to the required authentication mechanism or modification of parameters of the current authentication mechanism. The machine learning strategies, in its turn, first learn the baseline behavior of the device to detect deviations from that pattern, adapting the authentication mechanisms.

Those systems evaluates changes in one or more factors to trigger the adaptation process. Some systems employ context as their adaptation factor, changing the authentication mechanism as the device moves from location to location [6]. Other systems employ risk perception as their adaptation factor, adapting when it detects changes in the risk level. Risk is connected to location, network traffic, and messages sent and/or received by the device [7]. Thus, the systems react to variations in those factors and changes the authentication method accordingly, ranging from not authentication in low risk or safe location to the highest authentication strength in high risk or unsafe locations.

However, adaptive authentication systems disregard social trust, derived from the relationship between devices [8]. In addition, some exhibit a centralized architecture – preventing autonomous operation – and do not scale as the devices move across locations and domains. Hence, an adaptive authentication system demand an scalable and autonomous architecture to handle the authentication process and to provide autonomous operation. Moreover, the solutions need to adapt to different contexts and device's capabilities in order to offer a suitable adaptation. Though, it is crucial for IoT to employ systems able to manage adaptive authentication through their relationships and capabilities for more robust management.

This work proposes a system for adaptive authentication management, supported by social trust and policies. The system, called GALENA (*mana**G**ement of **A**daptive authentication based on po**L**ici**E**s a**N**d soci**A**l trust*), seeks to determine the most appropriate authentication profile to perform authentication between devices. It uses social trust, calculated from the sociability between devices, as an input to the adaptation system. In addition to social trust, the system uses policies to help choose the appropriate authentication mechanism. This paper is organized as follows: Section II discusses the related work. Section III defines some assumptions taken by GALENA. Section IV describes the GALENA components and their operation. Section V presents conclusions.

## II. Related Works

Several authors in the literature have explored forms of adaptive authentication employing policies such as [6], [7]. However there are gaps to be explored such as the use of social trust as an adaptation factor. In [7], authors propose an adaptive authentication system for SDN-IoT networks in order to offer context-aware security. The system determines the risk associated to each context based on that context's attack model and then selects a suitable policy in order to reach that context's required security level. Despite this, the system depends of a pre-register phase where symmetrical security keys are negotiated for context transfer. In [6] authors proposed the EDAS system (*Autonomic Event-Driven Adaptive Security*). It evaluates the risk, derived from events reported by the devices, in order to adapt. The system employs policies to account for user preferences, devices' capabilities and security metrics. However, the centralization exhibited by EDAS might incur in scalability challenges. Also, it assumes events are transferred securely between participants and EDAS.

Trust has been studied in IoT in service selection and composition. In [9], authors proposed an trust management system as a service (TaaS) that is a cloud service which stores data about reputation of devices. TaaS employs social trust in order to evaluate other devices and compose and require services from them. Despite that, TaaS relies on a centralized service and does not allow for autonomous trust evaluation. In [10], authors employ context-based trust for service selection in a system called DATM. It employs social relations – Communities of Interest – to compartmentalize devices' behavior and compare them among different contexts. However, DATM does not allow for autonomous operation as it relies on one or more trust providers to centrally store trust values for the system.

Thus, we argue that the adaptive authentication systems should be capable of acting in an autonomous and distributed way among devices, by employing suitable adaptation factors, such as social trust. These solutions, while adapting the authentication process, should not yield additional overhead and should consider the devices' capabilities.

## III. System Model

This section shows an overview of the IoT network, communication and social models upon which the proposal executes. The network and communication models are responsible for connecting IoT devices and how they authenticate. The social models details the devices' social behavior.

**Network model:** An IoT network composed of devices identified by $D = \{d_1, d_2, d_3, ..., d_j\}$, which $d_j \in D$. Each device $d_j$ has an unique identifier ($Id$). Devices offer and take services $s \in S = \{s_1, s_2, ..., s_j\}$ from each other, mainly autonomously. Furthermore, the characteristics of the devices' surroundings determine if they are static or have mobility, the processing restriction they have, and their services.

**Communication model:** Communication among devices occurs over an wireless medium on a shared asynchronous channel. Devices exchange messages using 6LoWPAN over IEEE 802.15.4. They form an ad hoc network and authenticate with each other in order to interact. Devices have a set of authentication mechanisms $m \in M = \{m_1, m_2, ..., m_j\}$ according to their communication and processing power. A profile $P_i^m$ groups the specific configuration of a mechanism ($m$) sequentially ($i$).

**Social behavior:** Devices inherit social characteristics from their owners and also create them autonomously, according to SIoT paradigm. Social characteristics considered are the following ones: Co-location object relationship (C-LOR), Co-work object relationship (C-WOR) and, Social object relationship (SOR), as defined by [8]. Devices have a C-LOR relation if they are located in the same context, but do not necessarily provide the same services. If they provide the same service, then they create a C-WOR relation. Lastly, devices create a SOR relation when they interact, continuously or sporadically.

## IV. GALENA System

This section introduces the adaptive authentication management system called GALENA (*Mana**G**ement of **A**daptive Authentication Based on Po**L**ici**E**s a**N**d Soci**A**l Trust*). Its architecture comprises two subsystems, **Discovery Management (SDM)** and **Authentication Management (SAM)** and an **Context Service (SCON)**, as seen in Fig. 1. They act jointly to guarantee discovery of devices and services, and also adaptive authentication. The Discovery Management locate devices and determines their services; the Authentication Management controls the adaptive authentication process; and the Context Service determines the context for the other subsystems.

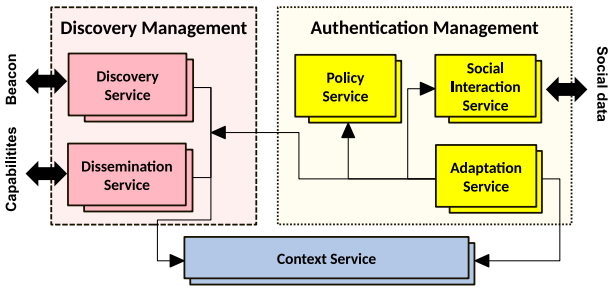


Fig. 1. The GALENA Architecture

The **SCON** is responsible for context determination. It acquires the context by means of GNSS (Global Navigation Satellite System) systems, triangulation, trilateration, etc. The context can have a semantic definition, either automatically from online location services or from user interaction, generating contexts such as "work" or "school". After being acquired, SCON passes the context information to the other services to take action based on them.

The **SDM** controls the discovery of neighboring devices and also builds a mapping between locations, services, and devices that can offer them. SDM comprises the Discovery Service (SDES) and Dissemination Service (SDIS). SDES discovers (or remembers) devices in the context, determined by SCON. After that, the service uses discovery mechanisms such

as mDNS and DNS-SD to discover devices' capabilities and their services. SDIS disseminates the device's authentication capabilities and services. The **SAM** manages social interaction with other devices, authentication policies and adaptive authentication. SAM interacts socially with other devices trough the Social Interaction Service (SSOC) that gathers and disseminates social data about other devices. Also, it responds to other devices' social data requests. The Policy Service (SPOL) manage the device's authentication policies. Finally, the Adaptation Service (SADPT) queries the policies, social data and context. Then, it determines which authentication mechanism should be used.

### A. Discovery and Dissemination

Devices need to discover neighboring devices and their services to interact. Algorithm 1 describes the discovery and dissemination process. Initially, SDES periodically announces the presence of the device using procedure `AnnouncePresence`. When it receives another device's announce, it registers the device as a neighbor in that specific context (procedure `ReceiveAnnounce`). Then, SDIS queries that device about its authentication capabilities and services and updates its neighbor list (procedure `RequireCapabilities`). A device disseminates its authentication capabilities and services using procedure `AnswerCapabilitiesRequest`. Those services also periodically empties their neighbors list and their capabilities to save space and eliminate information about low frequented contexts (procedure `PeriodicCleanUp`).

**Algorithm 1:** Discovery and Dissemination

```
1  procedure AnnouncePresence()
2      NeighborList ← 0
3      while True do
4          SendAnnounce()
5          WaitInterval ()
6  procedure ReceiveAnnounce()
7      NeighborId ← GetId()
8      Context ← GetContext()
9      NeighborList[Context] ← NeighborList[Context] ∪ NeighborId
10     RequireCapabilities(NeighborId)
11 procedure RequireCapabilities(NeighborId)
12     Context ← GetContext()
13     NeighborCapabilities[Context][NeighborId] ←
         RequireNeighborCapabilities(NeighborId)
14 procedure AnswerCapabilitiesRequest()
15     SendServicesAndAuthenticationMechanisms()
16 procedure PeriodicCleanUp()
17     Contexts ← GetAllContexts()
18     forall Context in Contexts do
19         NeighborList[Context] ← 0
20         NeighborCapabilitites[Context] ← 0
```

### B. Adaptive Authentication

To authenticate with another device in a context, SADPT queries SPOL about that context's policies. Policies in GALENA encode authentication rules as defined by the user or the device administrator. A policy $\mathcal{P}_j$ takes the devices' $Id$, its supported authentication mechanisms, its social trust value, and the context to determine an authentication profile. The tuple $\langle Id, AuthCapabilities, \mathcal{T}_{Id}, context\rangle = P_i^m$ defines a policy. Function $\mathcal{F}(attribute, value)$ filter the $attribute$ with $value$. An example of a policy can be seen as follows: $\mathcal{P}_1 = \langle \mathcal{F}(Id, *), \{PUF, RSA\},$

$$\mathcal{T}_{Id} > 0.5, \mathcal{F}(context, \text{“}school''\rangle = P_1^{RSA}$$

This policy applies to every device ($\mathcal{F}(Id, *)$), with authentication capabilities PUF and RSA. Furthermore, it only applies to context *school*. Another restriction lies on the social trust value of the device ($\mathcal{T}_{Id}$), where it should be higher than *0.5*. Finally, the policy, when applied, determines the usage of the authentication mechanism RSA.

### C. Social Trust

SSOC calculates the social trust using Eq. 1 where LOR and WOR values related to the C-LOR and C-WOR social relations. SSOC derives those values by their similarity for WOR, or normalized distance, for LOR. Trust values varies from 0 to 1 and the values $\alpha, \beta, \gamma$ form a constraint where their sum must remain unitary.

$$\mathcal{T} = \alpha * LOR + \beta * WOR + \gamma * SOR \tag{1}$$

SSOC determines the SOR value using Eq. 2 where the ratio $\mu/\pi$ quantifies the success ratio when interacting with that device. Expression $e^{-\lambda_d(t_{now}-t)}$ expresses the decay in social trust as time passes where $-\lambda_d$ represents the decay rate and $(t_{now} - t)$ represents time variation between the first interaction and this interaction. $R$ quantifies the average of recommendations from other devices. Finally, $\delta$ balances between direct trust, first part of sum, and indirect trust, second part of sum. SSOC evaluates the equations when it interacts with a target device, and when a neighboring device asks for its trust over a third device.

$$SOR = \delta * \left(\frac{\mu}{\pi}\right) * e^{-\lambda_d(t_{now}-t)} + (1 - \delta) * R \tag{2}$$

After SADPT obtains the trust values from SSOC, the policies from SPOL and the context from SCON, then it applies the policies and decide which authentication mechanism or specific configuration to employ in the authentication process for that context (procedures `DecidePolicy` and `AuthUsing` in Algorithm 2).

**Algorithm 2:** Adaptive Authentication

```
1  procedure DecidePolicy(NeighborId)
2      Context ← GetContext()
3      Policies ← GetPolicies(Context)
4      Capabilities ← NeighborCapabilities[Context][NeighborId]
5      SocialTrust ← T_Id
6      M ← DecidePolicy(NeighborId, Capabilities, SocialTrust,
         Context, Policies)
7      AuthUsing (M)
```

### D. Operation

We illustrate the operation of system in a smart city setting with multiple applications such as Smart Home, Intelligent Transportation Systems and Smart Street Lighting, whose devices are embedded in objects and can be fixed or mobile. Interaction between devices happens in different times and locations. Devices in the transmission radius of others exchange messages in order to negotiate services. Fig. 2 illustrates how GALENA operates and selects the most suitable authentication mechanism for a given context. The wireless signals mean devices within the transmission radius of each other and thus apt to exchange control messages about their services. Each device carries its identifier $Id$ and a set of supported authentication mechanisms $m \in M$. Mechanisms $m_1$, $m_2$ and $m_3$ correspond to three authentication mechanisms, respectively.

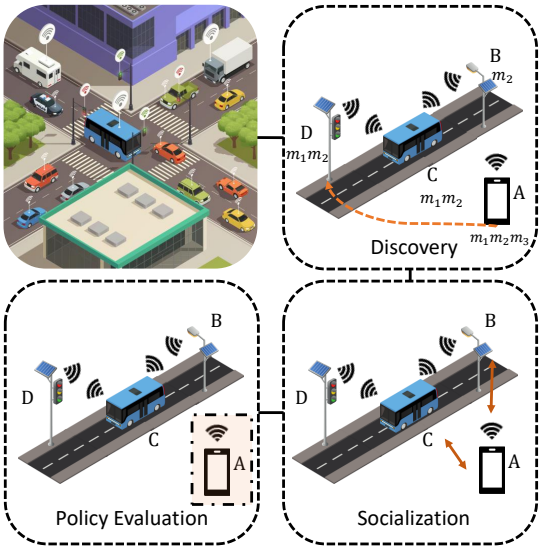


Fig. 2. GALENA Operation

GALENA operates in three phases: Discovery, Socialization, Policy Evaluation followed by Authentication, which GALENA does not directly participate. In the Discovery phase, devices discover others in proximity and devices $A$, $B$, $C$ and $D$ become aware of each other and services available. During this phase, device $A$ autonomously decides to request a service from device $D$. In the next phase, Socialization, $A$ does not have a direct social trust for device $D$, as they have not interacted before. To derive a social trust value, it inquiries the other devices ($B$ and $C$) about their trust over $D$, which they answer as 0.7 and 0.8, respectively. $A$ then calculates the overall recommendation $R$ as 0.75. Furthermore, $A$ and $D$ do not offer the same set of services, then $WOR = 0$ and are in close proximity, leading $LOR = 0.95$. $A$ has the following parameters configured for Eq 1 and Eq. 2: $\alpha = 0.5$, $\beta = 0$, $\gamma = 0.5$ and $\delta = 0.5$, leaving the equations as $\mathcal{T} = 0.5 * 0.95 + 0.5 * (0 + (1 - 0.5) * 0.75) = 0.66$, left-hand side of Eq. 2 equals to zero as the devices have not interacted.

After the Socialization phase, Policy Evaluation happens. Device $A$ gets its policies related to the "street" context, resulting in the following policy: $\mathcal{P}_2 = \langle \mathcal{F}(Id, *), \{m_1, m_2\},$

$$\mathcal{T}_{Id} > 0.65, \mathcal{F}(context, \text{“}street\text{”})\rangle = P_2^{ECC}$$

$A$ selects the profile $P_2^{ECC}$ as the means of authentication, given $D$'s characteristics matches the policy. This process happens in parallel on Device $D$. Both devices then authenticate using the selected mechanism and exchange services. This way, GALENA allows devices to autonomously use an authentication mechanism suitable to the context and perceived social relation. Moreover, it enables for customization and enforcement authentication mechanisms preferences.

## V. Discussion and Conclusion

We argue that IoT devices need to employ suitable authentication mechanisms while they roam across different parts of the network. Also, that adaptive authentication systems should employ perceptions related to the environment and the relationships in it, such as social relations among devices. This work presented GALENA for adaptive authentication in IoT. It determines the appropriate authentication mechanism for the authentication process based on the perceived social trust between two devices. The system also employs policies to encode adaptation preferences of the authentication process. Those approaches allows the assessment of the behavior of other devices and the analysis of the level of trust for device authentication, providing robustness in service relations. As future work, we intend to evaluate the convergence and accuracy of the proposed social trust protocol in relation to ground truth and its resiliency against bad-mouthing attacks.

## References


[1] G. Gardašević, M. Veletić, N. Maletić, D. Vasiljević, I. Radusinović, S. Tomović, and M. Radonjić, "The IoT architectural framework, design issues and application domains," *Wireless Personal Communications*, vol. 92, no. 1, pp. 127–148, Oct. 2016.

[2] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer Networks*, vol. 54, no. 15, Oct. 2010.

[3] M. El-hajj, A. Fadlallah, M. Chamoun, and A. Serhrouchni, "A survey of internet of things (IoT) authentication schemes," *Sensors*, vol. 19, no. 5, p. 1141, Mar. 2019.

[4] P. Arias-Cabarcos, C. Krupitzer, and C. Becker, "A survey on adaptive authentication," *ACM CSUR*, vol. 52, no. 4, pp. 1–30, Sep. 2019.

[5] A. Huertas Celdrán, M. Gil Pérez, F. J. García Clemente, and G. Martínez Pérez, "Towards the autonomous provision of self-protection capabilities in 5G networks," *Journal of Ambient Intelligence and Humanized Computing*, vol. 10, no. 12, pp. 4707–4720, 2019.

[6] W. Aman and E. Snekkenes, "EDAS: An evaluation prototype for autonomic event-driven adaptive security in the internet of things," *Future Internet*, vol. 7, no. 4, pp. 225–256, Jul. 2015.

[7] T. Sylla, M. A. Chalouf, F. Krief, and K. Samaké, "Towards a context-aware security and privacy as a service in the internet of things," in *IFIP Information Security Theory and Practice*, 2020, pp. 240–252.

[8] L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The social internet of things (SIoT) - When social networks meet the internet of things: Concept, architecture and network characterization," *Computer Networks*, vol. 56, no. 16, pp. 3594–3608, 2012.

[9] I.-R. Chen, J. Guo, D.-C. Wang, J. J. Tsai, H. Al-Hamadi, and I. You, "Trust as a Service for IoT Service Management in Smart Cities," in *IEEE HPCC/SmartCity/DSS*. IEEE, jun 2018, pp. 1358–1365.

[10] B. Jafarian, N. Yazdani, and M. S. Haghighi, "Discrimination-aware trust management for social internet of things," *Computer Networks*, vol. 178, p. 107254, Sep. 2020.