Adaptive and composite privacy and security mechanism for IoT communication

Swaminathan Seetharaman
DMTS-Senior Member
Wipro Limited, India
Swaminathan.Seetharaman@wipro.com

Sudipta Ghosh
Head-Intellectual Property Management
Wipro Limited, India
sudipta.sghosh@wipro.com

***Abstract*— With billions of connected devices expected in near future, the number and nature of IoT networks and their various interactions is certain to grow rapidly. As a result, the need for security and privacy of IoT networks during such interactions is a subject of major interest. Security & privacy related aspects need to take into consideration the context and purpose of such diverse types of interactions apart from the requirement of authentication and authorization of IoT networks, and dynamic perception-based interactions. Further, the security and privacy needs may be dynamic based on the involved parties and their dynamic relationships, and changes in the environment during or across such interactions. In this paper we propose a context-aware, purpose-aware, dynamic, adaptive and composite privacy and security mechanism that is risk averse and selectively sharing information as desired. Sample use cases and practical deployment-related aspects are presented that would enable our proposed mechanism to be employed in real-world IoT networks.**

Keywords—Security and privacy; context-aware; purpose-aware; IoT communication; dynamic and adaptive; composite privacy and security

I. INTRODUCTION

IoT devices and networks are growing exponentially in different forms around us all over the world, and would soon become ubiquitous. There are different types of IoT networks based on function/purpose, user, topology, etc. These include connected cars, home automation, remote tracking and surveillance, manufacturing and factory process automation, wearables and wireless body area networks (WBANs), smart cities, unmanned vehicle networks used for e.g., for military and security purposes, smart grid and smart meters, etc. There are different facets to IoT and IoT communication including device identification mechanisms, energy-aware operation and communication, device capabilities, criticality of events, IoT device and IoT network mobility, AAA (authentication authorization and accounting) aspects, privacy and security. If we look at security and privacy, different kinds of IoT networks have specific privacy and security needs. Further, IoT devices and networks need to perform appropriate actions depending on the context, environment and purpose in order to fulfill service or functional requirements, and such actions should conform to the security and privacy needs of the involved entities and networks.

Let us now look at two use cases to illustrate the privacy and security aspects in more detail.

A. Privacy: Wireless-Body-Area-Network

Let us consider an IoT WBAN. The network may be acquiring and processing a large amount of information from the user's body, some of which is strictly private for the individual user, some which may be private under specific scenarios and some which can be public. Examples of highly private information include biometric data such as heartbeat, pulse rate that is captured by the wearable devices, as well as medical history and health conditions of the user.

Some of the user's information may be disclosed conditionally and/or selectively by the IoT network to external networks (IoT or otherwise) and applications – e.g., to pre-authorized persons such as doctors, laboratories, insurance companies, etc. Further, the extent of information sharing depends on factors such as the recipient of the information (e.g., human user or machine, authorized or not authorized), context and purpose for which the information is being shared (emergency, health check), environment (e.g., public place, doctor's cabin), means of communication (e.g., IoT local protocols such as LoRA [1], DASH7 [2], Bluetooth [3] or protocols such as Wi Fi), etc. For instance, in case of a health emergency, relevant information about the patient's critical parameters and medical history may be shared to a set of doctors without any detailed authentication/authorization procedures in a private and secured manner so that sensitive information does not fall into the wrong hands. However, biometric footprint, medical data, etc. should be shared in phases in a private and secured manner as the interaction progresses. So we see that the privacy and security aspects depend on the context, purpose and intent of the interacting IoT network(s). Further secure communication (disclosure, negotiation, information exchange) also means access, transmission, storage and further use of information in an appropriately secure manner.

B. Disclosure & Security: Car-IoT

Consider a scenario involving the IoT network of a connected car (Car-IoT) of a particular car owner. As the Car-IoT enters a gas station, it has to register its presence by disclosing basic identity and some minimal information. The gas station's IoT network, in turn, could expose information about all services offered by the gas-station. Once the Car-IoT decides to avail specific service(s), then both parties would have to disclose further details in order to negotiate and fulfill the service(s). Such disclosure could involve authentication and

authorization steps (for availing the service, payment), and several rounds of query-responses and negotiations, most of them in an automated manner without human intervention. In this scenario also we see that the disclosure is based on need, function and should be controlled accordingly. For instance, the Car-IoT could disclose information such as fuel level and car health if it wanted to obtain service from the gas station's IoT. Subsequently, it may provide owner details for authorization and payment. While leaving the gas station, the Car-IoT could interact with neighboring cars to obtain information about the road, traffic and other safety-related information without any detailed authentication/ authorization steps to enable instantaneous exchange of relevant information.

Further, if the Car-IoT develops a greater trust during the course of initial interactions with the gas station's IoT, it may decide to expose information about other needs and interest in value-added services that can be catered by the gas-station's IoT. Subsequently, during further interactions, if the Car-IoT determines that the environment is not secure or it gets external inputs that the experience with the gas station's IoT was not good, the Car-IoT may decide to limit its information exposure.

Hence the privacy and security requirement, i.e., extent of information exposure and the manner in which information is exchanged could change dynamically during an ongoing interaction. Thus there is a need to dynamically adapt the privacy and security settings taking into consideration the context, purpose, collective past experiences and other factors.

The rest of this paper is organized as follows: Section II examines related work in this area, Section III describes our proposed mechanism, Section IV presents an interaction illustration, Section V briefly discusses some of the important deployability considerations, Section VI describes future work in this exciting area, and Section VII presents the conclusions.

II. RELATED WORK

Perera et al [4] state that security, privacy and trust are challenges in context-aware computing which will increase for IoT communication, and security and privacy aspects in IoT have to be addressed at each layer of the protocol stack.

Skarmeta et al [5] propose a distributed capability-based access control mechanism based on digitally signed capability-token. The capability-token contains access rights and the means to authenticate the requestor. The proposed mechanism is static and hence unsuitable for changing context and purpose, and for heterogeneous IoT networks consisting of devices with varying capabilities. Gusmeroli et al [6] also propose a capability-based access control mechanism in which the capability directly identifies the resource(s), the subject to which the rights have been granted, the granted rights, and the authorization chain. However, the proposed mechanism requires issuing capabilities to all subjects, and is not suitable for dynamically changing security and privacy requirements during progressive interactions of IoT networks. Mahalle et al's [7] Identity Authentication and Capability Based Access Control (IACAC) also has similar limitations as other capability-based access control mechanisms mentioned above.

Xin Huang et al [8] propose a context-aware k-anonymity policy that anonymizes the identifiers of the data record/user so that it is not distinguishable from other users except when required. This addresses the privacy aspect in a context-aware manner. However, privacy settings are not dynamically adapted during an interaction with another entity. Security-related aspects of IoT communication are also not addressed.

Pohls et al [9] propose a framework for security, privacy and trust for smart city IoT networks. The proposed mechanism includes continuous monitoring and management of security events using an adapted form of the PRRS [10] platform, and provides automated adaptation of deployed security mechanisms to enable reconfigurations due to change in context. However, the mechanism requires explicit reporting of context change, and handles only a limited set of context parameters which is not sufficient to address interactions spanning vastly heterogeneous IoT networks. The proposed privacy and trust mechanism fails to adapt during the course of an interaction.

GAMBAS [11] suggests a policy-based privacy mechanism that enables secure exchange of information after authentication, key exchange, etc. However, it does not address the dynamic changes in privacy & security requirements during the course of an IoT interaction. Role Based Access (RBAC) as suggested in Ferraiolo et al [12] can be adapted for IoT networks for privacy and security requirements. However, such an access does not address the dynamic privacy and security requirements during the course of IoT interaction.

Sarkar et al [13] propose a distributed layered architecture for IoT in which the Security Management (SM) module supports modeling, specification, and enforcement of security policies. The modeling is done using the collection of interrelated metamodels to represent the data, identities, context, roles, structure and behavior. The collection of metamodels and runtime components used in the SM is called SecKit ([14], [15]). The security policy rules are specified using parametrized templates to fulfill the privacy & security needs using an event condition action (ECA) structure. However, [13], [14], [15] fail to address dynamically changing privacy and security requirements during an IoT interaction.

Neisse et al [16] propose a context-aware and trust-based security & privacy framework in which security policies are implemented as ECA rules. However, the proposed framework does not dynamically adapt to changes in context, trust-level, environment, etc. during the interaction. The framework will also encounter limitations in scalability and deployability when faced with new/unknown service-oriented and inter-IoT interaction scenarios without any human intervention.

Gessner et al [17] propose a security architecture for authorization, authentication, and privacy based on trust and reputation for IoT networks. However, it does not address dynamic adaptations of the privacy & security mechanism as the interaction progresses. Further, it fails to provide any corrective mechanism in case of incorrect handling leading to critical risk condition. Peer-to-peer information collection and processing for trust and reputation computation may not scalable as the number of parties grow.

Existing mechanisms fail to provide dynamic, adaptive, context and purpose aware composite privacy and security framework that is risk averse and adaptive during interaction.

III. PROPOSED PRIVACY AND SECURITY MECHANISM

We present a context-aware, purpose-aware, dynamic, adaptive and composite privacy and security mechanism. It is based on the architectural principles proposed in [18]. The following terms are defined to be used in the rest of this paper.

- Perception: Is formed by an entity with regards to the set of possible interactions with a second entity, based on its own experience, information from other sources and collective perception. Perception is typically structured information. Perception can evolve before, during and after an interaction.
- Filter: Is a mechanism that determines the extent of information to be allowed to pass through. It is a set of rules and thresholds that will be applied on the messages / contents that are being passed through the filter. Filter can be uni-directional or bi-directional.
- Engagement: Represents an interaction session for an IoT network with a second party involving a network (IoT or otherwise) that is interested to obtain or deliver one or more services, exchange information, etc.

A. *Overview*

The network architecture illustrated in Fig. 1 is based on what has been proposed in [18]. The main components are:

IoT Gateway: Handles IoT network-specific aspects such as IoT-function, the IoT network components' identity, capability topology, etc., relevant information of neighboring IoT gateways, intra-IoT network communication aspects, etc.

Interconnect Gateway (ICG): Handles all aspects of inter-IoT communication including managing the communication channels towards IoT Gateway and MC cloud, session and service management, security and privacy, identity management, policy formulation and application, etc.

MC Cloud: The MC cloud represents the macro-cellular network (MCN) and its connectivity to other networks.

IoT Management Application (IoTMA): Manages the IoT network functions and policies.

IoT Consumer Application: An application that makes use of information from one or more IoT devices and IoT networks to provide service(s) to the user, IoT network, or other entities.

External Application: Any service-provider or third-party application that may interact with the IoT network.

Perception Management Entity (PME): This is a new entity for collecting perception-related inputs from different sources, organizing and managing the same, and providing relevant inputs upon request from the ICG. The PME could be present inside the MC Cloud or can be connected to the MC Cloud.

The PME provides inputs to the IoT Gateway about the trust rank of the ICG which it uses during selection of the appropriate ICG. Similarly, the IoTMA provides inputs about the trust rank of the IoT Gateway.

When an IoT network interacts with a second party, it forms an initial perception based on collective past experience. This is then used to decide whether to continue the interaction, and form a working perception based on the information received so far and the current context. As the interaction progresses, the working perception is adapted, and the purpose, need and interest levels are ascertained to decide whether to engage with the second party. When deciding to engage with the second party, an engagement perception is formed. Continuous monitoring of the engagement and appropriate refinement of the engagement perception happens during the engagement. When the engagement ends, a closing perception is formed. We will now take a closer look at the ICG architecture before diving deep into the proposed mechanism of providing security and privacy for an engagement.

B. *ICG Architecture*

The ICG architecture shown in Fig. 2 is based on [18]. There are 3 main sub-systems in the ICG – the IoT gateway interface sub-system that handles communications with the IoT network via the IoT gateway, the Macro-Cellular Network (MCN Interface) that handles communications with the macro/core networks and the central Management and Control sub-system (MCSS) responsible for Session and Service Management, handling of policies, management of identities, and handling administrative and security functions. The

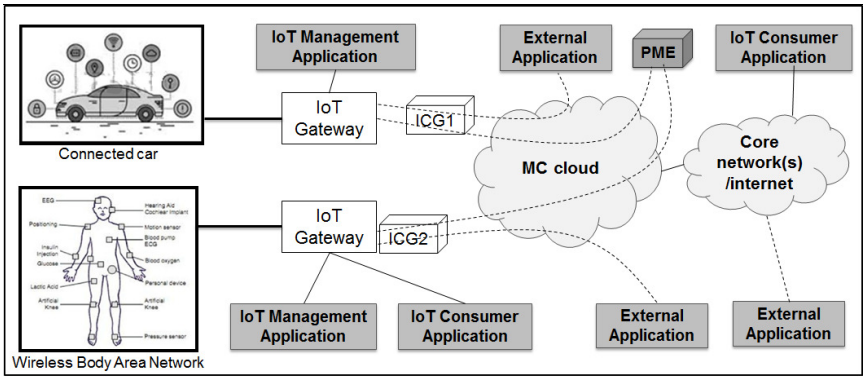

Fig. 1. Network-level view of IoT and applications

functions performed by the MCSS components for privacy and security are explained below.

1) Administration and Security (ADM & SEC)

a) Gathers perception related information from MC Cloud (e.g., stored in a PME) and passes it to the IoT Gateway at the initiation of communication, or based on request from IoT Gateway.

b) Based on information from IoT gateway, determines the mechanism(s) to ensure security of the communication channel and the communication content (e.g., encryption, authentication, etc.).

2) Communication module (CM)

a) Applies the relevant ICG filter for an engagement. This means that any information received/sent not passing through the filter are dropped/discarded, appropriate policy updates are made, and security violations reported to the relevant entities (Session and Service Management module, user, central repository, operator, etc.).

b) Takes specific actions based on request from IoT Gateway.

3) Session & Service Management (SSM)

a) Forms ICG Filter based on perception input (specific/general) from Policy Management module, MC Cloud and on specific request from the IoT gateway.

b) Modifies the Filter for exceptional situations when the CM takes specific action that needs alteration of Filter.

4) Policy Management

a) Updates policy based on information received from the operator, MC cloud, and CM.

a) Provides relevant perception related inputs to SSM.

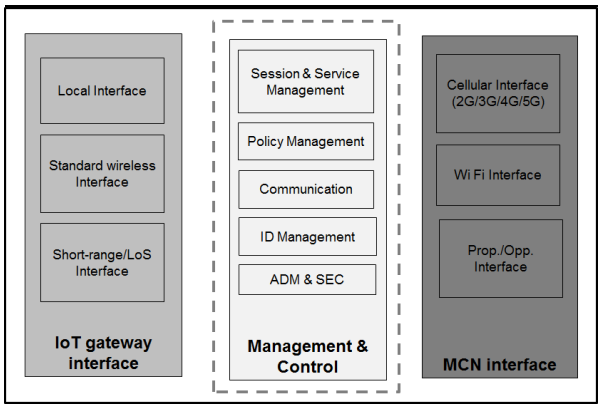

Fig. 2. ICG Architecture

C. *Functioning of the Proposed Mechanism*

The functioning of the proposed mechanism from the IoT network perspective is shown in Fig. 3. The actions indicated below are performed by the IoT Gateway in conjunction with IoT Management Application unless explicitly stated otherwise. The steps are explained below.

- Detect communication requirement: This step may involve discovery of an IoT network, a service or an IoT application, an incoming request for communication from another entity.
- Whether to communicate?: An initial perception is formed based on own perception and collective perception, and the security threat/risk level of the communication is ascertained. Based on initial perception and security threat(s), a decision on whether to communicate is taken. If it is decided not to communicate, stop the communication, update local database, and send relevant info to the ICG.
- Determine purpose of communication: Obtain relevant purpose-related inputs from second party or third party sources. Subsequently validate the inputs against locally stored memory (past engagements, transactions) and the globally stored data, and form a consolidated view about the purpose.
- Determine perception, need and trust level: Form a working perception from initial perception and adapt it based on the scenario, environment, etc. as appropriate. Determine the communication need based on the information received, function of the IoT network, and current context including the environment. Determine trust level of the communicating entity based on local info as well as external inputs (ICG, PME).
- Am I interested to communicate?: Based on the purpose, need, working perception and trust determined as explained above, decide whether the IoT network is interested to communicate further. If it is decided not to communicate, stop the communication, update local database, and send relevant info to ICG.
- Determine extent of information exposure: Set the appropriate security and privacy filter based on perception and purpose.
- Share allowed information: Pass the information through the filters set above, and share the information that emerges out of the filter. The ICG also has a separate filter which may further restrict information sharing for any communication happening via the ICG.
- Analyze responses and information received, and refine perception: Analyze all the information and response(s) (or lack thereof) received till now, and refine the working perception accordingly to make it more accurate.
- Does it address my need?: Based on the analysis above, determine whether the intended need is addressed (and to what extent). If the intended need is addressed, then go to the next step, else stop the communication, update local database, and send relevant info to the ICG.
- Determine interest level: Determine the interest level which is a combination of extent of need fulfillment and the perception formed about the communicating entity (i.e., the security, privacy and trust aspects).

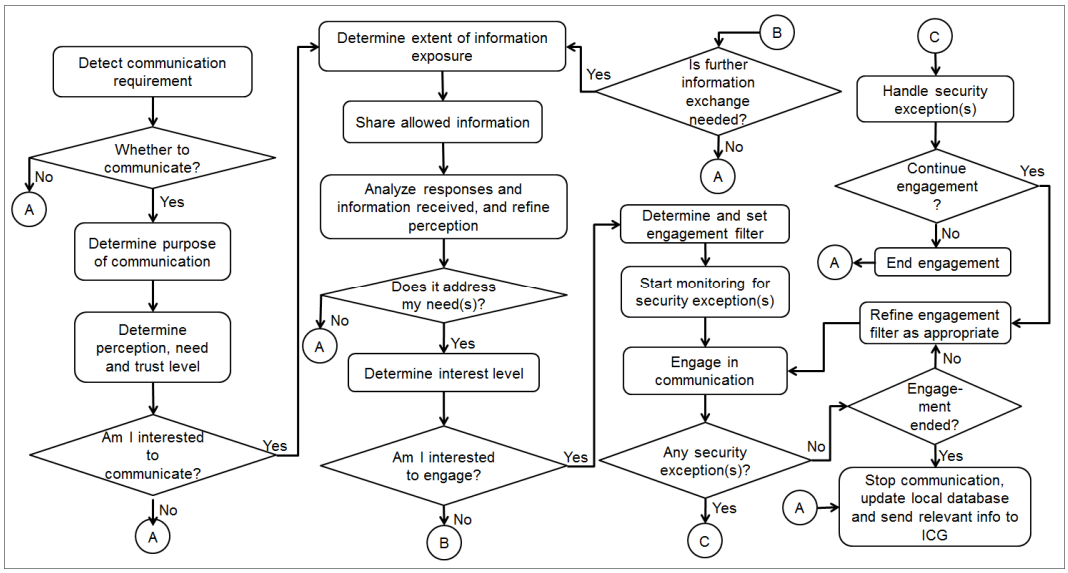

Fig. 3. Flowchart illustrating the functioning of the proposed mechanism

- Am I interested to engage?: Determine if interest level is above the interest level threshold or not. If yes, then go to the step 'Determine and set engagement filter', if no, go to the next step below.
- Is further information exchange needed?: Check whether further information exchange is required to ascertain accurately the extent of need fulfilment and/or forming a more accurate perception. If yes, then go to step 'Determine extent of information exposure', and the cycle continues until adequate information is obtained to take a final decision. If no, then stop the communication, update local database, and send relevant info to the ICG.
- Determine and set engagement filter: Form an engagement perception based on working perception, interest and purpose. Determine the filter to be used for the engagement, and set the appropriate filter.
- Start monitoring for security exceptions: Start monitoring for any security exceptions. This involves real-time analysis of information exchange based on perception, filter, history of engagement with the specific entity or similar entities, specific context or similar contexts. If required, the IoT Gateway may also consult the ICG or MC cloud in some situations.
- Engage: Start the requested transaction with the peer entity, share required information, and provide/ consume one or more services.
- Any security exception(s)?: Upon encountering security exception(s), assess the impact and also send appropriate information to the ICG. If there is no security exception, then continue the engagement and execute the 'Engagement ended' step.
- Continue engagement?: Determine whether the engagement can be continued. If yes, then go to the next step. If no, then end engagement, update local database, and send relevant info to the ICG.
- Refine engagement filter as appropriate: Adjust the engagement filter levels as appropriate and use the adjusted filter for further communication in the engagement. Continue engagement(go to Engage step).
- Engagement ended?: Periodically determine if the engagement has ended if there is no explicit trigger to end the engagement. If the engagement has not ended, then using relevant aspects of the communication up to now execute 'Refine engagement filter as appropriate' step. If the engagement has ended, then go to next step.
- Stop communication, update local database and send relevant information to the ICG: This step is self-explanatory. The locally stored information and the information sent to the ICG shall be used by the IoT network and the ICG for all future engagements.

D. *Perception Lifecycle*

Let us take a look at the perception lifecycle during the course of the engagement setup and progress as described above. Fig. 4 provides a simplified view of the states in the IoT Gateway's perception lifecycle. The states and state transitions from each state in the perception lifecycle are explained below:

1) Unknown: This is the starting state with no historical data, i.e., a clean slate. Transitions from this state are:

a) When triggered by a need to communicate, this state transitions to 'Initial Perception' state.

2) Initial Perception: An initial perception is formed in this state upon detection of a communication need. The initial perception is formed based on own perception and collective perception. Own perception is obtained from local perception stored based on the communicating entity or a similar entity.

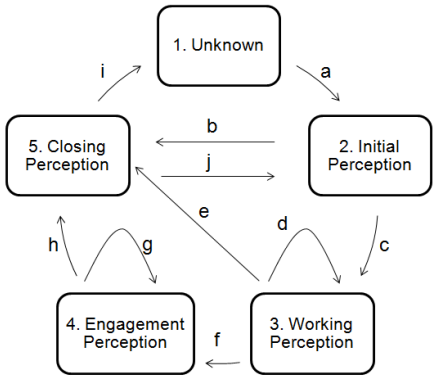

Fig. 4. IoT Gateway perception lifecycle

Collective perception about the identified party or similar parties is obtained from local cache, or by requesting the ICG and/or PME for relevant inputs. When transitioning from 'Unknown' state, an initial perception is formed based on collective perception alone. When transitioning from 'Closing Perception' state, an additional input for forming the initial perception is the own perception (stored in Closing Perception state). The state transitions are:

b) When it is decided not to communicate based on the initial perception, this state transitions to 'Closing Perception' state.

c) When it is decided to communicated further based on the initial perception, this state transitions to 'Working Perception' state.

3) Working Perception: A working perception is formed in this state by adapting initial perception to the current scenario taking into account the the communicating entity's identity, information received up to now from the communicating entity, environment, historical data about similar communication with the same or similar entities, etc. While continuing the interaction to determine the need, purpose and interest level to engage with the communicating entity, continuous and appropriate refinements will be made to the working perception. Working perception is initial perception customized to the current interaction. Transitions include:

d) This transition denotes the continuous refinement of working perception based on the information exchanged up to now, environment changes, and any external inputs.

e) At any point during the communication, if it is decided not to continue further with the communication, this state transitions to 'Closing Perception' state.

f) Upon determining that the need will be fulfilled and the interest level to engage is higher than the threshold, this state transitions to the 'Engagement Perception' state.

4) Engagement Perception: In this state, an engagement perception is formed/refined for continuing with the engagement. The engagament perception is the working perception customized to the current engagement taking into account interest, purpose, environment, etc. Transitions are:

(g) This is a continuous transition during the life-time of the engagement, and involves regular refinement until the engagement ends or until forced termination of engagement.

(h) Upon termination of the engagement (e.g., due to to a security exception), or when the engagement ends, this state transitions to the 'Closing Perception' state.

5) Closing Perception: In this state, all relevant data is updated locally, and a closing perception is formed about the communicating entity based on experience during the current engagement. When transitioning to this state on normal ending of the engagement or forced engagement termination from 'Engagement Perception' state, the closing perception is formed based on objectives met, security incidents, etc. When transitioning from 'Initial Perception' or 'Working Perception' states, the closing perception is formed based on the information exchange and context of the engagement request. The transitions from this state are:

i) This transition indicates the flushing of closing perception after a pre-defined time, or forcefully by the user or policy triggers.

j) This transition occurs upon detection of a need to communicate with an entity where a closing perception exists – this closing perception will be a key input in determining the initial perception for the new communication request.

During the course of the information exchange while the engagement is being established or is in progress, the IoT network and the ICG may exchange relevant information periodically or on occurrence of exceptions based on which they may adapt their perception and filters.

Fig. 5 illustrates the perception lifecycle of the ICG. It encompasses a wider view, and is not as fine-grained as the IoT Gateway's perception lifecycle, and evolves less frequently. The states and state transitions are explained below.

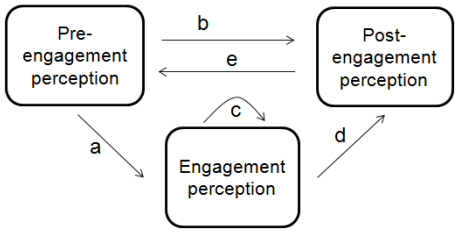

Fig. 5. ICG perception lifecycle

Pre-engagement perception (PREP): This is the perception that is formed based on earlier engagements involving the same or similar entities (if available) and taking into consideration the environment, and information received from external sources (PME, other ICGs), etc. before the engagement starts. Based on this setting, the engagement is allowed to be initiated.

Engagement perception (ENGP): This is the perception that is formed from PREP as the engagement commences. It changes during the engagement based on any abnormal situations, notifications from the PME or updates based on inputs from other ongoing engagements via the same ICG. The changes in ENGP are less frequent as compared to changes in the Engagement Perception of the IoT Gateway.

Post-engagement perception (POSTP): This is the perception that is formed at the end of the engagement, based on inputs from the IoT Gateway and locally stored data.

IV. INTERACTION ILLUSTRATION

Using the mechanism above, we will now analyze the evolution of the filters in a practical engagement involving two IoT networks. This will serve to illustrate how the proposed mechanism operates in real-world IoT communication scenarios. Let us assume that the first IoT network is interested to obtain a service that is provided by the second IoT network. Fig. 6 illustrates how the communication filters in the IoT Gateway and the ICG are adapted dynamically during the course of an engagement. The ICG and IoT Gateway filters are formed as explained below.

- ICG Filter: Formed based on perception input (specific /general) from PME, and upon specific request from the IoT gateway. ICG filter is concerned with the network-level communication aspects, blacklisting of some entity or a class of entities, types of communication, security exceptions, etc. Once formed, it is mostly static for a single engagement with a few exceptions.
- IoT Gateway Filter: Formed based on perception input (specific/general) from PME, and based on own perception formed earlier. IoT Gateway Filter is highly dynamic, and changes continuously during the engagement based on the information exchanged, changes in the environment, security exceptions, etc.

Let us assume a common three-point scale for both the ICG and IoT Gateway filter setting. In real-world scenarios, the filter levels can be highly granular with different scales for the ICG and the IoT Gateway.

1) Restrictive: This filter setting corresponds to a low level of trust and/or security level of the environment, allows only the essential information exchange to happen.

2) Medium: This filter setting corresponds to a moderate level of trust and/or security level of the environment, or only a moderate understanding of the true purpose.

3) Transparent: This filter setting corresponds to a high level of trust, and a highly secure environment.

Let us further assume that the initial settings of the ICG Filter and the IoT Gateway filters are 'Transparent' and 'Medium' respectively. As the engagement progresses, this setting could evolve dynamically as illustrated below. Cases 1-3 are normal scenarios involving dynamic adaptations in a context and purpose-aware manner in the IoT Gateway filter settings based on the environment and/or the engagement with the remote entity.

- Case 1: Based on interaction with the remote entity, the IoT gateway views it as highly trusted, hence IoT Gateway filter setting changes to 'Transparent'.
- Case 2: The environment may be moderately secure and/or the interacting entity may only be trusted to some extent, so there is no change to the initial filter setting of ICG and IoT Gateway.
- Case 3: The environment may be unsecure, or the interacting entity may not be trusted, so the IoT Gateway filter setting alone changes to Restrictive.
- Cases 4-6: These are abnormal cases in which the ICG filter shrinks to Medium or Restrictive level when the engagement is in progress, perhaps due to some security exceptions, for e.g., not-allowed contents, unknown information, unexpected content format, change in identity/credentials of the peer, etc.

From the above illustration, we see that the security and privacy settings are adapted dynamically at the IoT Gateway level based on all IoT-network specific, engagement-context and purpose-specific aspects. At the ICG level, the dynamic adaptation is based on security exceptions and any external inputs received during the course of an engagement.

Thus the IoT communication can continue in a secure manner by adapting the communication characteristics and information exchanged to adjust to any changes in context, exceptional situations or any external inputs.

V. DEPLOYMENT CONSIDERATIONS

Some of the key practical deployment considerations are presented below:

1) Scope of ICG: ICG should not consider IoT-network

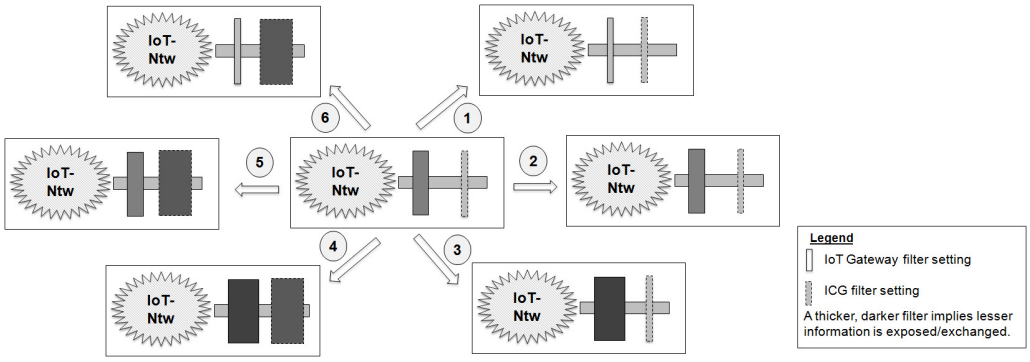

Fig. 6. Dynamic adaptation of communication filters during an IoT interaction

function specific aspects, as scalability and information consistency aspects will become an issue.

2) Latencies and overheads: Latencies and signaling overheads may be involved when the IoT Gateway interacts with ICG/PME often to obtain perception-related inputs. To overcome such overheads, purpose-based interaction and clear demarcation of local and global perception-related information should be implemented.

3) Inter-ICG information sharing: It would be useful if ICGs residing in an operator network can share information about their perceptions, so secure mechanisms of periodically sharing such information can be implemented.

4) Handling unknown situations: When handling unknown contexts and/or when the purpose cannot be determined accurately, decision regarding extent of further information sharing can be based on the risk appetite of the IoT user, network policies, history of known security attacks, etc.

5) Authentication and secure communication: Appropriate method(s) of authentication and secure communication should be employed when deploying our proposed mechanism.

6) PME placement: The PME might have to consist of (geographically) distributed instances at appropriate locations with caching and synchronization amongst them to make it scalable, highly available and robust against network failures.

VI. FUTURE WORK

In the security and privacy mechanism presented above, the filters in the IoT Gateway and ICG operate independent of each other, even though some of the filter settings could have been influenced by some common factors. It would be interesting to study if an alignment of the perceptions and hence a correlation of the IoT Gateway and ICG filters lead to a more intelligent, accurate and optimized handling of security and privacy needs.

Currently the IoT Gateway and ICG filters are stateless across engagements. Further work is required to assess the benefits of stateful filters across engagements (i.e., taking into account the last filter setting for a similar engagement), and the overheads involved. The security/privacy-related interactions between the IoT Gateway and ICG should be explored further for very short-lived engagements, and initial interactions with very low latency requirements (so whether to engage, and how much to expose require decision-making on-the-fly by the IoT gateway). We intend to implement our approach in a real-world setting for the two use cases described in this paper (connected cars and WBAN) and fine-tune the proposed mechanism to function better to enable wider deployability.

VII. CONCLUSIONS

IoT networks and their interactions to realize services those are new and even unimagined today is likely to proliferate in the years to come. Given this context, security and privacy aspects are important dimensions in present and more so in future IoT networks. As discussed in this paper, the security and privacy requirements will change depending on the context, purpose, etc., and will change dynamically during an engagement. We have proposed a context-aware, purpose-aware, dynamic, adaptive and composite privacy and security mechanism. The proposed mechanism is highly adaptive and scalable, and hence can fulfill the security and privacy requirements of almost any kind of real-world IoT network.

REFERENCES

[1] https://www.lora-alliance.org/What-Is-LoRa/Technology

[2] http://www.dash7-alliance.org/?product=dash7-alliance-protocol-specification-v1-0

[3] https://developer.bluetooth.org/TechnologyOverview/Pages/core-specification.aspx

[4] Perera, C., Zaslavsky, A., Christen, P., Georgakopoulos, D., "*Context Aware Computing for The Internet of Things: A Survey*", IEEE Communications Surveys and Tutorials, Volume 16, Issue 1, Feb 2014.

[5] Skarmeta, A.F., Hernández-Ramos, J.L., Moreno, M.V., "*A decentralized approach for Security and Privacy challenges in the Internet of Things*", 2014 IEEE World Forum on Internet of Things (WF-IoT), March 2014.

[6] Gusmeroli, S., Piccione, S., Rotondi, D., "*IoT Access Control Issues: A Capability Based Approach*", 6th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, July 2012.

[7] P. N. Mahalle, B. Anggorojati, N. R. Prasad, and R. Prasad, "*Identity authentication and capability based access control (iacac) for the internet of things*", Journal of Cyber Security and Mobility, vol. 1, no. 4, pp. 309–348, 2013.

[8] Xin Huang, Rong Fu, Bangdao Chen, Tingting Zhang, Roscoe, A.W., "*User interactive Internet of things privacy preserved access control*", International Conference for Internet Technology And Secured Transactions, December 2012.

[9] Pohls, H.C., Angelakis, V., Suppan, S., Fischer, K., Oikonomou, G., Tragos, E.Z., Diaz Rodriguez, R., Mouroutis, T., "*RERUM: Building a Reliable IoT upon Privacy- and Security- enabled Smart Objects*", IEEE Wireless Communications and Networking Conference Workshops (WCNCW), April 2014.

[10] A. Garcia, et al., "*FI-WARE Security: Future Internet Security Core*" in 'Towards a Service-Based Internet', ser. Lecture Notes in Computer Science, vol. 6994. Springer Berlin Heidelberg, 2011, pp. 144–152.

[11] Generic Adaptive Middleware for Behavior-driven Autonomous Services (GAMBAS) Consortium, "*Privacy Preservation Specification 1*", Public deliverable D3.1.1, September 2012, Available online: http://www.gambas-ict.eu/download/D3.1.1-Privacy-Preservation-Specification-1.pdf?attredirects=0&d=1.

[12] D.F. Ferraiolo, D.R Kuhn: Role-Based Access Control. 15th National Computer Security Conference. pp. 554–563, October 1992.

[13] Sarkar, C., Nambi, A.U.S.N., Prasad, R.V., Rahim, A., Neisse, R., Baldini, G., "*DIAT: A Scalable Distributed Architecture for IoT*", IEEE Internet of Things Journal, Vol. 2, No. 3, June 2015.

[14] Neisse R, et al., "*SecKit: A Model-based Security Toolkit for the Internet of Things*", Computers & Security, June 2015, http://dx.doi.org/10.1016/j.cose.2015.06.002.

[15] Neisse, R., Steri, G., Baldini, G., "*Enforcement of Security Policy Rules for the Internet of Things*", IEEE 10th Int. Conf. on Wireless and Mobile Computing, Networking and Communications (WiMob), October 2014.

[16] Neisse, R., Steri, G., Baldini, G., Tragos, E., Nai Fovino, I., Botterman, M., "*Dynamic Context-Aware Scalable and Trust-based IoT Security, Privacy Framework*", Book chapter in Internet of Things - From Research and Innovation to Market Deployment, IERC Cluster Book, 2014, pp.199-224.

[17] Gessner, D., Olivereau, A., Segura, A.S., Serbanati, A., "*Trustworthy Infrastructure Services for a Secure and Privacy-respecting Internet of Things*", 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 2012.

[18] Ghosh, S., Seetharaman, S., "*Mechanism for adaptive and context-aware inter-IoT communication",* IEEE International Conference on Advanced Networks and Telecommunication Systems (ANTS), December 2015, in press.