Cyber-entity Security in the Internet of Things

Huansheng Ning[1], *Senior Member, IEEE*, Hong Liu, *Student Member, IEEE*,
and Laurence T. Yang[2], *Member, IEEE*

Abstract: The Internet of Things (IoT) is an emerging future network paradigm, and aims to achieve the interconnections among ubiquitous things among heterogeneous networks. During a physical-object being mapped as the corresponding cyber-entities, the across-space interactions bring unique security challenges to the cyber-entities in the IoT. In this article, we consider the Unit and Ubiquitous IoT (U2IoT) to address the cyber security issues, present the recommended security approaches according to the cyber-entity activity cycle, and further establish a secure interaction solution for different interaction scenarios with both security and privacy considerations.

Keywords: Internet of Things (IoT), authentication, cyber-entity, physical-object, security.

1 Introduction

The Internet of Things (IoT) is emerging as an attractive network paradigm, in which a physical-object is mapped as one or more cyber-entities for pervasive interconnections among heterogeneous networks. The cyber-entities play pivotal roles to achieve connectivity with the associated physical-objects during the interactions, in which multiple cyber-physical-social characteristics are assigned to the cyber-entities in the across-space contexts.

Recent studies have been worked on the IoT system models [1, 2], and security issues are raised to bring intense speculations. Existing security works mainly include systemic security frameworks and strategies [3,4], networks based cryptographic security mechanisms [5], and IoT applications oriented security solutions [6,7,8]. Accordingly, the related works can be classified into system security, network security, and application security. *System security* mainly considers an overall IoT system to identify security challenges, to design security frameworks, and to provide security guidelines; *Network security* focuses on sensing and networking based communications (e.g., radio frequency identification (RFID), and wireless sensor networks (WSNs)) to design cryptographic algorithms, including key distribution, authentication, and access control; *Application security* serves for IoT applications to address the security issues according to scenario requirements. Towards above security aspects, the cyber-entities are suffering from severe challenges during the secure interconnections.

- *Expanding cyber-entity domains:* Along with physical-objects' being mapped into the cyber space, more cyber-entities are emerging for pervasive networking and communicating. The scope of the cyber-entities in the IoT is expanded compared with that in the Internet, and security problems subsequently become more complicated;

- *Dynamic cyber-entity activity cycle:* Cyber-entities may exist in a dynamic activity cycle with different duties considerations. For instance, a cyber-entity has completed its activity cycle in a scenario, and becomes a temporarily unavailable resource. While, the cyber-entity may be still in active in other scenarios, and such inconsistent activity cycles bring challenges towards the security approaches;

- *Heterogeneous cyber-entity interactions:* The interactions among the cyber-entities are not only the cyber-physical issues, and the associated social attributes become particularly important for the across-space interactions. The individual-aware and group-aware social relationships among cyber-entities should be considered during the secure interactions.

H. Ning and H. Liu are with School of Electronic and Information Engineering, Beihang University, Beijing, China (e-mail: ninghuansheng@buaa.edu.cn; liuhongler@ee.buaa.edu.cn).
L. T. Yang is with School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan, China, and also with the Department of Computer Science, St. Francis Xavier University, Antigonish, Canada (e-mail: ltyang@stfx.ca).

Digital Object Indentifier 10.1109/MC.2013.74 0018-9162/$26.00 2013 IEEE

Particularly, a human-social inspired Unit and Ubiquitous IoT (U2IoT) architecture has been presented [2], and the novel IoT model realizes the interconnections across the physical, cyber, and social spaces. Based on the aforementioned challenges, this article will address the cyber-entity security issues based on the U2IoT architecture.

2 System Architecture and the Cyber-entity Domains

2.1 Overview of the Unit and Ubiquitous IoT (U2IoT)

The U2IoT architecture refers to Unit IoT and Ubiquitous IoT. The Unit IoT is a single IoT application, and the Ubiquitous IoT includes multiple interrelated Unit IoTs with the region/industry/nation considerations. Fig. 1 shows a layered U2IoT system model, including the perception layer, network layer, and application layer.

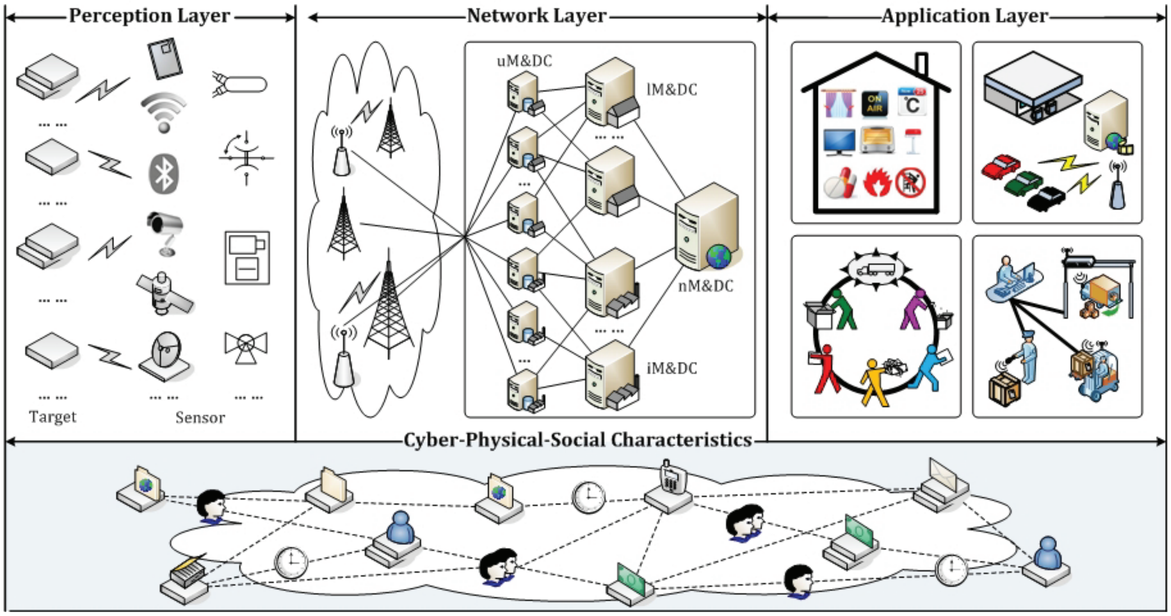


Figure 1: The layered U2IoT system model.

The perception layer realizes to convert the physical-objects into the cyber-entities, and comprises the generalized sensors to perform target identification and physical-objects' cyberlization. The sensing techniques mainly include ZigBee, RFID, Wi-Fi, Bluetooth, infrared induction, global positioning system (GPS), and radar. Note that the mechanical/electronic actuators (e.g., valve, and switch) can be connected with the sensors to execute the appointed instructions.

The network layer includes multiple network components (e.g., interfaces, routers, and gateways) and communication channels. Note that management and data centers act as network nodes for communications. Thereinto, a unit management and data center (i.e., uM&DC) may be under the direct or indirect jurisdictions of the local, industrial, and national management and data centers (i.e., lM&DC, iM&DC, and nM&DC). Heterogeneous network configurations may be established based on the Internet, WSNs, mobile communication networks, and telecommunication networks. This layer ensures the reliable data transmission by applying the secure data coding, fusion, mining, and aggregation algorithms, and realizes the interconnection among the heterogeneous networks.

The application layer provides functional services to support IoT applications, and covers Local IoTs, Industrial IoTs, and National IoTs, in which lM&DC, iM&DC, and nM&DC respectively provide data management. Concretely, a Local IoT realizes interconnections among Unit IoTs in a geographical region; an Industrial IoT manages Unit IoTs in an industry or industry chain (e.g., transportation, and telecommunications); and a National IoT is the collection of multiple Local IoTs and Industrial IoTs within a nation. Moreover, service integration, transnational supervision, and international coordination are

Digital Object Indentifier 10.1109/MC.2013.74 0018-9162/$26.00 2013 IEEE

considered in this layer. The standard protocols (e.g., constrained application protocol (CoAP), and wireless application protocol (WAP)) and service composition technologies (e.g., service oriented architecture, and cloud computing) can be applied in IoT applications (e.g., smart home, and smart grid).

In the U2IoT, ubiquitous things mainly exist in two forms: physical-objects and cyber-entities. A physical-object refers to a thing with an objective existence, and a cyber-entity is an abstraction to carry information (e.g., session identifier, and social relationship) during interconnections. Multiple cyber-physical-social characteristics are assigned to the cyber-entities.

1. *Space-time consistency:* A cyber-entity can interact with other cyber-entities at any time, at any place, and in any mode. The cyber-entity may freely enter or leave the interactions without influencing the ongoing sessions. The space-time registration, synchronization, and correlation should be considered in the heterogeneous networks.

2. *Multi-identity co-existence:* A cyber-entity may have multi-identity status, including a core identity and other temporary or assistant identities according to its applications. Such a multi-identity can be represented by identifiers or non-identifiers. For instance, a tagged item is assigned with an identifier (e.g., electronic product code (EPC)) for identification in RFID systems, and a person owns biological characteristics (e.g., fingerprint, and iris) as non-identifier for unique recognition. In other scenarios, non-unique identifiers and non-identifiers can be jointly used for thing representation.

3. *Dynamic interaction:* A cyber-entity can adapt for dynamic environments according to the heterogeneous networks, and the cyber-entity is directly or indirectly interrelated with each other, and ubiquitous interactions are established to support further intelligent data processing.

4. *Social awareness:* A cyber-entity should be assigned with full-fledged social attributes, which describe the social relationships with the associated physical-objects. The social attributes consider the aspects such as ownership control management, affiliation relationship modeling, and behavior formalization. Note that the social awareness aims to present individual-aware and group-aware social relationships among the cyber-entities.

2.2 The Cyber-entity Domains in the U2IoT

Architecturally, the U2IoT includes three main cyber-entity domains: unit domain, ubiquitous domain, and logical domain.

2.2.1 Unit Dmain

The unit domain corresponds with the cyber-entities in the Unit IoT, and is formed by the cyber-targets, cyber-sensors, and uM&DCs. This domain achieves continuously real-time target data collection, environmental monitoring, and basic information management.

The cyber-targets mainly refer to two aspects: one is the sensed data (e.g., temperature, gas sensitivity, and blood pressure) of the physical/chemical/biological parameters in the surrounding environments; and the other is the available data (e.g., quick response code) attached in the physical-objects.

The cyber-sensors have the active and passive modes according to whether there is an in-built power source. The active cyber-sensors can actively probe the physical-objects for data acquisition, such as radars, cameras, and thermocouples. The passive cyber-sensors capture data without actively challenging the physical-objects. Typical passive cyber-sensors include Infrared sensors, and resistance temperature detectors (RTDs). Note that the two types of cyber-sensors may apply the same sensing technology in different applications. For instance, an active 2.4 GHz RFID tag has an on-board battery for identification in electronic toll collection (ETC), and a passive 13.56 MHz RFID tag is triggered by the backscattered signals for supply chain management.

The uM&DCs act as the intermediate network components, and establish the interconnections between the unit and ubiquitous domains. They can manage the interactions of the cyber-targets and cyber-sensors, perform data storage/fusion/mining on the sensed data, and extract advanced knowledge to provide intelligent services, decision support, and real-time event response for the Unit IoT.

Digital Object Indentifier 10.1109/MC.2013.74 0018-9162/$26.00 2013 IEEE

2.2.2 Ubiquitous Domain

The ubiquitous domain as the collection of multiple unit domains, is the core of the Ubiquitous IoT. In this domain, the cyber-entities mainly include diverse management and data centers (i.e., lM&DC, iM&DC, and nM&DC) to perform management on the Local IoTs, Industrial IoTs, and National IoTs.

The lM&DCs manage the loosely coupled and geographically dispersed Local IoTs in the grid mode, in which grid computing can be introduced for infrastructure management. Meanwhile, the independent lM&DCs can be organized in the cluster structure for data collection around different regions.

The iM&DCs manage the industries or industry chains oriented Industrial IoTs in the hierarchical mode. The related Industrial IoTs are correlated with particular relationships, and multi-agents based collaborative management can be applied for the layered data aggregation among different industries.

The nM&DCs are usually act by the utilities to supervise Local IoTs and Industrial IoTs within a nation, and to perform arbitration when there is a dispute. An nM&DC may interact with the affiliated iM&DCs/lM&DCs, or other uM&DCs to provide coordination services.

2.2.3 Logical Domain

According to the cyber-entities' interaction coverage, the logical domain is defined to represent the relationships through the unit domain and ubiquitous domain. The logical domain refers to the relationships of independent, affiliation, and inclusive & exclusive.

- *Independent* indicates that cyber-entities' interaction coverage has no obvious dependence. For instance, in the smart home, the ambient brightness and fuel gas density are independent cyber-targets. Accordingly, the light-sensitive sensor and gas detector have relatively independent environment monitoring functions.

- *Affiliation* refers to that a cyber-entity's interaction coverage is affiliated with another cyber-entity's coverage, and includes two aspects: attribution and hereditament. *Attribution* means that a cyber-entity belongs to another cyber-entity, and *hereditament* means that a cyber-entity owns inherent attributes of another cyber-entity, and also has other distinctive attributes. For instance, in the smart city, a home monitoring center is under the jurisdiction of its default community monitoring center, which represents the attribution relationship. In the smart grid, a power line sensor and a smart meter as different cyber-sensors, both inherit the common sensing functions for data collection and transmission, and also have dissimilar characteristics according to the practical environments.

- *Inclusive & Exclusive* means that cyber-entities' interaction coverage is inter-relevant in the forms of overlapped or non-overlapped relationships, and logical operators (e.g., AND, OR, and NOT) can be applied for relationship descriptions. For instance, in the supply chain, there are multiple participants (e.g., manufacturer, carrier, and retailer), which manage the corresponding authorized items, and may have different access authorities on a certain item. Similarly, the item may be accessed by an only appointed participant, and other participants cannot obtain any information.

3 Cyber Security Challenges in the U2IoT

3.1 Enhanced Cyber Security Requirements

The enhanced cyber security requirements should be considered in the U2IoT, including CIA Triad, authority, non-repudiation, and privacy preservation.

CIA Triad considers the basic requirements on data confidentiality, integrity, and availability. It should be ensured that a physical-object cannot be unauthorizedly correlated with the corresponding cyber-entities and social attributes.

Authority mainly refers to authentication and authorization. Besides, advanced requirements should be considered.

Digital Object Indentifier 10.1109/MC.2013.74 0018-9162/$26.00 2013 IEEE

- *Multi-access authority:* Single sign-on (SSO) can be applied to achieve the compatible multi-access authority, by which a single authority action can obtain the associated access permission without repetitive verification;

- *Multi-semantic authority:* Multi-semantic based identification and verification should be established according to the heterogeneous networks.

Non-repudiation is traditionally to provide available proofs to prove the availability of a cyber-entity's behaviors that can be presented by a trusted third party. Additionally, non-repudiation should achieve the compatible social computing and behavior supervision for the cyber-entity's behaviors.

Privacy preservation aims to protect sensitive individual information, in which *transparency* and *traceability* should be considered to achieve privacy-utility tradeoff in the U2IoT. The former means that let a user know which cyber-entity owns the related data, and when/where/how the data has been used, and the latter means that let a cyber-entity know which networks and services it has even connected.

3.2 Security Attacks and System Vulnerabilities

In the U2IoT, main security attacks can be classified into four categories: gathering, imitation, blocking, and privacy attack. *Gathering* (e.g., skimming, tampering, eavesdropping, and traffic analysis) occurs when the data is collected via wired/wireless channels. *Imitation* (e.g., spoofing, cloning, and replay) owns the purpose of impersonation for an unauthorized access. *Blocking* (e.g., denial of service (DoS), jamming, and malware) refers to the communication and system interferences. *Privacy attack* means individual or group sensitive information disclosures. Note that such attacks may have correlations, such as a gathering attack may cause an imitation attack, and further lead to privacy exposure. Table I summarizes the typical security attacks and countermeasures. Moreover, the cyber-entities suffer from several vulnerabilities.

1. *Cyber-targets:* Dynamic participation and mobility bring new challenges for cyber-target identification, in which the major threats are data interception and identity forgery. For instance, in vehicle-to-grid (V2G) networks, a tagged battery vehicle's data may be illegally captured by adversaries, which can distort (e.g., insert, delete, and replace) data for cheating a power aggregator.

2. *Cyber-sensors:* The cyber-sensors are mainly resource-constrained devices with limited energy and storage. The adversaries may actively manipulate (e.g., misrepresent, and intercept) data, or passively monitor (e.g., sniffing, and eavesdrop) data transmission. For instance, in ZigBee based WSNs, the sensor nodes and sink nodes are dynamically self-organized in a multi-hop manner, and the malicious nodes may be embedded into the area to communicate with the neighbor nodes for data collusion.

3. *Management and data centers:* The management and data centers are confronted the similar threats as these in the Internet, such as DoS/Distributed DoS (DDoS) may cause system resource exhaustion. The newly emerging data management modes (e.g., cloud storage, and collaborative big data) may cause privacy disclosure. For instance, data sharing is achieved to support intelligent decision, but the shared data may be abused to injure individual privacy.

4. *Networks:* The connections between the cyber-targets and cyber-sensors are mainly based on wireless communication channels, and such open interfaces may have inherent defects. For instance, in Bluetooth based networks, a mobile phone's multimedia data is transmitted via the peer-to-peer mode, in which frequency-hopping spread spectrum (FHSS) is applied for data protection, but the eavesdropping still occurs during the data transmission. The communications among different M&DCs are mainly based on mobile communication networks, telecommunication networks, and the Internet. The next generation networking standards and technologies (e.g., LTE-Advanced, WirelessMAN-Advanced, and IPv6) are still in the infancy, and robust mechanisms should be designed for reliable communications.

Digital Object Indentifier 10.1109/MC.2013.74 0018-9162/$26.00 2013 IEEE

Table 1: The typical security attacks and countermeasures

	Attacks	Impacts	Countermeasures
Gathering	Skimming*	Quick read the transmitted messages for data abuse.	Encryption, and steganography.
	Tampering†	Data modification and deletion for deliberate data destruction and corruption.	Hash function, cyclic redundancy check (CRC), and message authentication code (MAC).
	Eavesdropping*	Collect and detect the exchanged messages.	Encryption, identity-based authentication, and concealed data aggregation (CDA).
	Traffic analysis*	Monitor the exchanged data to determine traffic patterns.	Network forensics, and misbehavior detection.
Imitation	Spoofing*,†	Impersonate as a legal data source to obtain an access authority for identity cheating.	Identity-based authentication, key distribution, Internet protocol security (IPSec), and digital signature (e.g., ElGamal).
	Cloning*	Duplicate and re-write valid data into an equivalent entity.	Physically unclonable function (PUF).
	Replay*	Record and store the previously transmitted data for data repeating or delaying in the current session.	Timestamp, time synchronization, pseudo-random number, session identifier, and serial number.
Blocking	DoS‡	Flood data streams to interfere communication channels, and to exhaust system resources.	Firewall, router control, resource multiplication, distributed packet filtering, dynamic en-route filtering, and aggregate congestion control.
	Jamming‡	Electromagnetic interference or interdiction by using the same frequency band wireless signals.	Anti-jamming, active jamming, and Faraday cage.
	Malware*,‡	Apply viruses, worms, Trojan horses, spyware, dishonest adware and other programs to interfere with system.	Anti-virus program, firewall, and intrusion detection.
Privacy	Individual privacy*	Derive an individual user's locations, preferences, behaviors, and other private information, and correlate the sensitive data with the user's real identity.	Aggregated proof, anonymous data transmission, CDA, and advanced digital signature (e.g., blind, group, and ring signatures).
	Group privacy*	Evaluate a group user's commercial interests, and deduce its affiliated commercial espionage and trust domains.	Selective disclosure, data distortion, and data equivocation.

The possible security consequences: ∗: Loss of data confidentiality; †: Loss of data integrity; ‡: Loss of data availability.

4 Cyber-entity Activity Cycle Based Security Approaches

During a cyber-entity existing in the cyber space to establish interactions, it has an activity cycle, including the pre-active, active, and post-active phases. The mentioned "active" is defined according to a cyber-entity's interactive session. Concretely, *pre-active phase* refers to that the cyber-entity is in the preliminary status before launching a session (e.g., network accessing, and service addressing), *active phase* means that the cyber-entity is in the ongoing session, and *post-active phase* indicates that the cyber-entity is in the inactive status after the current session.

4.1 Security Approaches for the Pre-active Phase

4.1.1 Key Distribution

Key distribution includes the symmetric and asymmetric key agreements for two or more cyber-entities. Thereinto, cryptographic primitives (e.g., identity-based cryptography, bilinear Diffie-Hellman problem, and Tate pairing) can be applied for key distribution. Additionally, group key agreement can be adopted by multiple cyber-entities to establish dynamic keys, and the shortest path tree routing mode and multi-path key mode are suitable for the heterogeneous and cross-layer communications. Meanwhile, quantum cryptography is a challenging topic, in which Greenberger-Horne-Zeilinger states is used for multi-entity key distribution.

4.2 Security Approaches for the Active Phase

4.2.1 Authentication

Authentication considers the validity of the interactive cyber-entities. Traditional authentications are mainly based on the pre-shared secrets and TTP, and improved authentications should fully consider the network features (e.g., heterogeneity, mobility, and scalability). Towards the authentication operators, ultra-lightweight algorithms such as bitwise operators, permutation, pseudo-random number can be applied by the resource-constrained devices; lightweight algorithms including hash, CRC, and MAC can be applied to provide enhanced security; and full-fledged encryption/signature algorithms can be used by databases. Meanwhile, the physical mechanisms (e.g., PUF) can be used for authentication, and an IP-based protocol (i.e., protocol for carrying authentication for network access (PANA)) has been standardized by IETF for network access authentication. Moreover, multi-cast message authentication and batch authentication become efficient for multiple cyber-entities' interactions.

4.2.2 Access Control

Access control refers to the authorization among different legal cyber-entities with the classified authorities on system resources. The hybrid mode can be established according to the access control paradigms (e.g., mandatory, discretionary, role-based, and attribute-based access control mechanisms). Additionally, semantic-based mode is feasible for the web services oriented networks, and trust-oriented mode is practicable for the virtualization of cyber-entities' behaviors with social attribute considerations. Meanwhile, conditional proxy re-encryption can be used to address the data sharing and data hiding in the cloud computing.

4.2.3 Secure Routing

Secure routing is traditionally applied along with the IPSec to achieve dynamic routing, and is becoming critical for mobile Ad hoc networks (MANETs). The multi-path routing and on-demand routing protocols can be applied in the heterogeneous sensing networks, and different routing schemes (e.g., tree-based, identity-based, and trust-based routing protocols) should be designed for secure data transmission.

4.2.4 Advanced Signature

Advanced signature algorithms mainly include blind, group, ring, and identity signature. Thereinto, proxy blind signature and partially blind signatures can use Bilinear maps for verification, and other encryption algorithms (e.g., elliptic curve cryptography) can also be used for signature generation. Additionally, certificateless signature has obvious advantages in computational cost, and knowledge based off-line signature can achieve perfect forward security.

4.2.5 Zero-knowledge Proof

Zero-knowledge proof is used in the interactions between a prover and a verifier without revealing any sensitive information, and it includes the interactive and noninteractive modes during identity verifications. Thereinto, the Σ-*protocol* with different composition modes (e.g., parallel, EQ, OR, and AND), can be

Digital Object Indentifier 10.1109/MC.2013.74 0018-9162/$26.00 2013 IEEE

applied for the aggregated proofs verification. Meanwhile, blind watermark technique is suitable for the zero-knowledge based verification in lightweight applications.

4.2.6 Data Aggregation

The data aggregation is originally to aggregate multiple sensing data by performing algebraic or statistical functions to establish a data set for transmission. Concealed data aggregation can provide privacy homomorphism encryption with additive homomorphism to achieve enhanced security. Additionally, the yoking-proofs or grouping-proofs can be regarded as data aggregation, which realize that sensing data is aggregated as a group for authentication. Meanwhile, the hierarchical data aggregation can be applied in the intra-networks and inter-networks, in which homomorphic encryption and signature algorithms can be jointly used to achieve data confidentiality and integrity.

4.3 Security Approaches for the Post-active Phase

4.3.1 Intrusion Detection

Intrusion detection detects the malicious attacks, and enables the systems and communications in a secure status. The adaptive network intrusion detection algorithms should be designed for the heterogeneous networks. Meanwhile, artificial immune and artificial neural networks can be introduced for the non-self identifications and real-time monitoring. Additionally, data mining techniques (e.g., feature selection and modeling) also provide assists to enhance unreliable node detection.

4.3.2 Intrusion Tolerance and Threshold Cryptography

Intrusion tolerance refers to secret sharing to distribute a secret among multiple cyber-entities, in which each cyber-entity is allocated a share of the secret. Note that intrusion tolerance and threshold cryptography realizes that multiple cyber-entities collectively participate into the secret management. Even in the case that a cyber-entity is temporarily inactive or perennially unavailable, other legal cyber-entities can also perform the normal interactions. Note that intrusion tolerance and threshold cryptography are usually used along with other cryptographic algorithms. For instance, dynamic group key agreement can apply threshold secret sharing to achieve key distribution among multiple cyber-entities, segmentation can be introduced into the overlay secret space for the distributed memory sharing, and hierarchical secret sharing scheme can be designed according to the hybrid network structures (e.g., multi-level, compartmented, and multi-partite). Moreover, fragmentation redundancy scattering can provide enhanced tolerance resilience, and dependable intrusion tolerance and hierarchical intrusion tolerance can be applied in the detection-triggered IoT applications.

5 The Secure Interaction Solution among the Cyber-entities

In this section, we consider the RFID based scenarios to introduce the secure interactions among the cyber-entities in the U2IoT. Here, the cyber-entities refer to a tag (i.e., *T*, as a cyber-target), a reader (i.e., *R*, as a cyber-sensor), a uM&DC (i.e., *uMC*), and a(n) lM&DC/iM&DC/nM&DC (i.e., *lMC*, *iMC*, and *nMC*). Note that $\{uMC_l, uMC_i\}$ respectively represent the corresponding uM&DCs with the default jurisdictions of *lMC* and *iMC*. According to the logical relationships among the cyber-entities, Fig. 2 illustrates the typical three interaction scenarios, and a secure interaction solution is proposed in Fig. 3.

Digital Object Indentifier 10.1109/MC.2013.74 0018-9162/$26.00 2013 IEEE

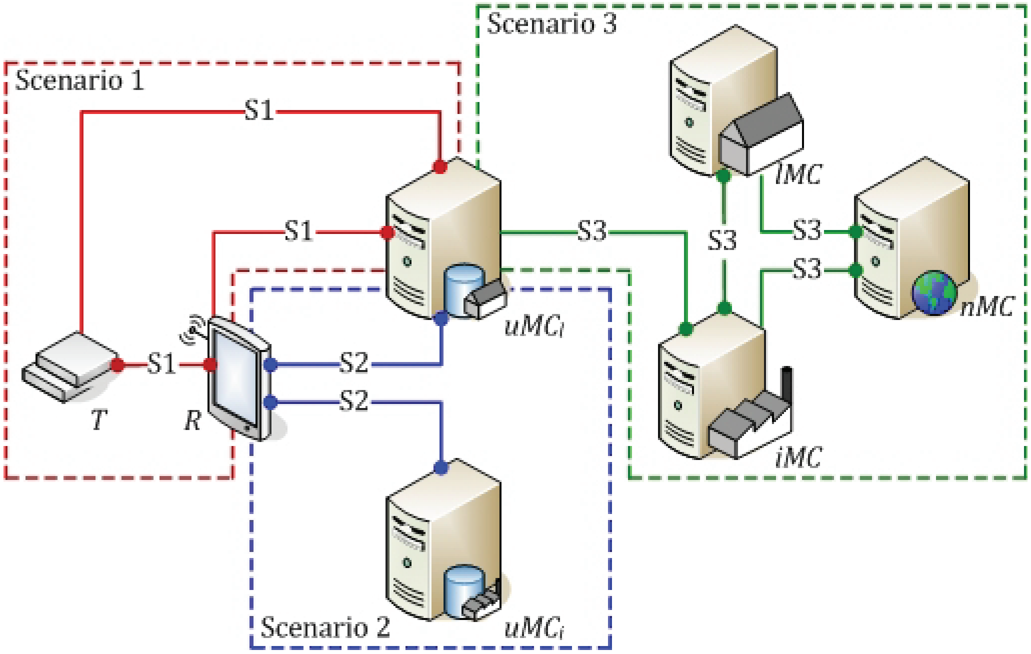


Figure 2: Three interaction scenarios among the cyber-entities.

Scenario 1: Secure Data Access Interaction considers an interaction in a Unit IoT, in which T and R establish mutual authentication, and uMC_l ensures that T and R are both legal cyber-entities. Here, $\{T, R\}$ are within uMC_l's coverage, and uMC_l as a trusted entity can access the sensed tag data for management.

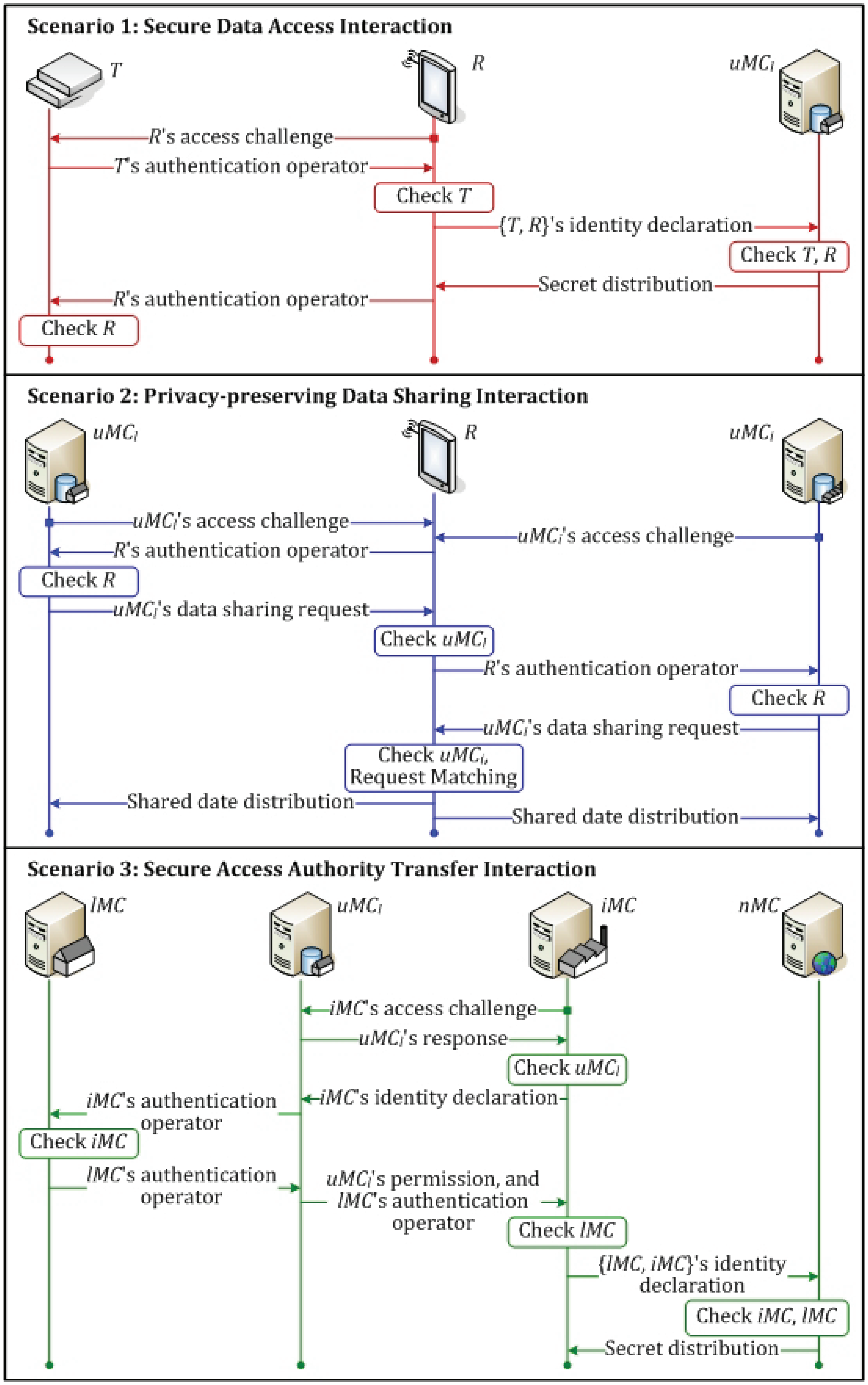
1. R generates an access challenge to query T, and T replies an authentication operator to R for verification. If T is legal, R will transmit $\{T, R\}$'s authentication operators to uMC_l for identify declaration;

2. uMC_l performs verifications on $\{T, R\}$. Upon uMC_l ascertaining their validity, uMC_l transmits a message to T for secret distribution. Then, R transmits an authentication operator to T for verification. If R is legal, $\{T, R\}$ will establish mutual trusts for secure data access.

Scenario 2: Privacy-preserving Data Sharing Interaction considers an interaction between a Local IoT and an Industrial IoT. Here, $\{uMC_l, uMC_i\}$ are respectively under the jurisdictions of Local IoT and Industrial IoT, and are assigned different access authorities on a certain R. It turns out that they have independent authorities to access R's data fields, and $\{uMC_l, uMC_i\}$ grant their own access authorities to each other without compromising the individual privacy.

1. $\{uMC_l, uMC_i\}$ successively transmits access challenges to R, and R establishes the simultaneous communications with uMC_l and uMC_i. R first transmits an authentication operator to uMC_l for verification. If R is legal, uMC_l will reply a data sharing request to R. Thereafter, R verifies uMC_l's validity to derive the private request;

2. Afterwards, R turns to communicate with uMC_i, and $\{R, uMC_i\}$ performs the similar operations (including $\{R, uMC_i\}$'s mutual verification, and uMC_i's data sharing request extraction). Till now, R has obtained $\{uMC_l, uMC_i\}$'s requests, and further performs request matching to ascertain whether $\{uMC_l, uMC_i\}$ have the same access desire on each other's data. If it holds, R will respectively transmit the shared data to uMC_l and uMC_i. Thus, privacy preservation is achieved that only in the case that both uMC_l and uMC_i have the matched data sharing requests, R will publish each other's sensitive data for data sharing. If there is no matched request, any irrelevant data will not be revealed.


Scenario 1: Secure Data Access Interaction
T
R
uMC_i
R's access challenge
T's authentication operator
Check T
{T, R}'s identity declaration
Check T, R
Secret distribution
R's authentication operator
Check R
Scenario 2: Privacy-preserving Data Sharing Interaction
uMC_i
R
uMC_j
uMC_i's access challenge
uMC_j's access challenge
R's authentication operator
Check R
uMC_i's data sharing request
Check uMC_i
R's authentication operator
Check R
uMC_j's data sharing request
Check uMC_j, Request Matching
Shared date distribution
Shared date distribution
Scenario 3: Secure Access Authority Transfer Interaction
lMC
uMC_i
iMC
nMC
iMC's access challenge
uMC_i's response
Check uMC_i
iMC's identity declaration
iMC's authentication operator
Check iMC
lMC's authentication operator
uMC_i's permission, and lMC's authentication operator
Check lMC
{lMC, iMC}'s identity declaration
Check iMC, lMC
Secret distribution

Digital Object Indentifier 10.1109/MC.2013.74 0018-9162/$26.00 2013 IEEE

Figure 3: The secure interaction solution for the three scenarios.

Scenario 3: Secure Access Authority Transfer Interaction considers an interaction among a Local IoT, an Industrial IoT, and the affiliated National IoT. Here, uMC_l is originally under *lMC*'s jurisdiction, and *iMC* wants to obtain the access authority of uMC_l from *lMC*. *lMC* transfers uMC_l's authority to *iMC* based on an agreement, and *nMC* performs final verifications on {*lMC*, *iMC*}.

1. *iMC* transmits an access challenge to uMC_l for authority transfer, and uMC_l responds an authentication operator for *iMC*'s verification. If uMC_l is legal, *iMC* will reply an operator for identity declaration;

2. uMC_l forwards *iMC*'s authentication operator to *lMC* for verification. If *iMC* is legal, *lMC* will reply an authentication operator to uMC_l. Thereafter, uMC_l generates authority permission, and forwards *lMC*'s authentication operator to *iMC* for verification. If *lMC* is legal, {*lMC*, *iMC*} will establish mutual agreement towards the authority transfer;

3. *iMC* transmits {*lMC*, *iMC*}'s authentication operators to *nMC* for identify declaration. When *nMC* ascertains the validity of {*lMC*, *iMC*}, *nMC* transmits a secret to *iMC* for secret distribution, which realizes the final authority registration in the top database.

Towards security analysis, the proposed solution satisfy the main security properties.

- *Session freshness:* The pseudo-random numbers and session-sensitive operators (e.g., session identifiers, and timestamps) can be applied as access challenge to ensure forward and backward unlinkability. An attacker regards the previous/subsequent sessions as random even if the cyber-entities have been corrupted.

- *Mutual authentication:* The mutual authentication is performed based on the pre-shared secrets (e.g., keys, and pseudonyms) and cryptographic algorithms to establish trusting relationships.

- *Hierarchical access control:* Different access authorities are assigned to cyber-entities to achieve classified security protection. For instance, uMC_l has a full authority on *T*, but *R* has a limited authority on *T*. Meanwhile, uMC_l and uMC_i have independent access authorities on *R*s data fields to avoid authority-exceeding violation.

- *Privacy preservation:* The anonymous data sharing requests are applied to hide the real access desires with privacy consideration. It realizes that only the matched access requests will launch the shared data distribution.

It indicates that the proposed solution addresses security and privacy issues during cyber interactions, and provides reliable authentications for the U2IoT.

6 Conclusions

In this article, we have identified the cyber-entity domains in the U2IoT, and presented the enhanced cyber security requirements. Accordingly, the security attacks and countermeasures are summarized, and the system vulnerabilities are analyzed according to the cyber-entities in the U2IoT. Meanwhile, we present the recommended security approaches towards a cyber-entity activity cycle, and propose a secure interaction solution to achieve security protection and privacy preservation.

Acknowledgment

This work is jointly funded by National Natural Science Foundation of China (NSFC) and Civil Aviation Administration of China (CAAC) (61079019).

References

[1] J. Ma, J. Wen, R. Huang, and B. Huang, "Cyber-Individual Meets Brain Informatics," *IEEE Intelligent Systems*, vol. 26, no. 5, pp. 30–37, 2011.

[2] H. Ning and Z. Wang, "Future Internet of Things Architecture: Like Mankind Neural System or Social Organization Framework? ," *IEEE Communications Letters*, vol. 15, no.4, pp. 461–463, 2011.
[3] R. Roman, P. Najera, and J. Lopez, "Securing the Internet of Things," *Computer*, vol. 44, no. 9, pp. 51–58, 2011.
[4] J. Pan, S. Paul, and R. Jain, "A Survey of the Research on Future Internet Architectures," *IEEE Communications Magazine*, vol. 49, no. 7, pp. 26–36, 2011.
[5] K. McCusker and N. E. O'Connor, "Low-Energy Symmetric Key Distribution in Wireless Sensor Networks," *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 3, pp. 363–376, 2011.
[6] D. He, C. Chen, S. Chan, Y. Zhang, J. Bu, and M. Guizani, "Secure Service Provision in Smart Grid Communications," *IEEE Communications Magazine*, vol. 50, no. 8, pp. 53–61, 2012.
[7] L. Zhou and H. C. Chao, "Multimedia Traffic Security Architecture for the Internet of Things," *IEEE Network*, vol. 25, no. 3, pp. 35–40, 2011.
[8] X. Li, R. Lu, X. Liang, X. Shen, J. Chen, and X. Lin, "Smart Community: An Internet of Things Application," *IEEE Communications Magazine*, vol. 49, no. 11, pp. 68–75, 2011.

Biographies

Huansheng Ning (M'10-SM'13) received a B.S. degree from Anhui University in 1996 and Ph.D. degree in Beihang University in 2001. Now he is an Associate Professor in School of Electronic and Information Engineering, Beihang University, China. His current research focuses on Internet of Things, aviation security, electromagnetic sensing and computing. He has published more than thirty papers in journals, international conferences/workshops.

Hong Liu (S'10) is currently working toward a Ph.D. degree at the School of Electronic and Information Engineering, Beihang University, China. She focuses on the security and privacy issues in radio frequency identification, vehicle-to-grid, and wireless machine-to-machine networks. Her research interests include authentication protocol design, and security formal modeling and analysis.

Laurence T. Yang (M'97) received a B.E. degree in computer science from Tsinghua University, China, and a Ph.D. degree in computer science from the University of Victoria, Canada. He is a professor in School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan, China, and also is computer science and the director of the Parallel and Distributed Computing Laboratory, and Embedded and Ubiquitous Computing Laboratory at St. Francis Xavier University, Canada. His research interests include high-performance computing and networking, embedded system, and ubiquitous/pervasive computing and intelligence. His research is supported by the National Sciences and Engineering Research Council, and the Canada Foundation for Innovation.

Digital Object Indentifier 10.1109/MC.2013.74 0018-9162/$26.00 2013 IEEE