RV College of Engineering®

UNIT –V
Security and Privacy in IoT

Prof. Narasimha Swamy S
Department of AIML
RV College of Engineering
Bengaluru-59

Go, Change the World

Content

→ Introduction

→ Security Challenges in U2IoT

→ The Security Framework for U2IoT

→ Hybrid Authentication and Hierarchical Authorization Scheme

→ Entity Activity Cycle–Based Security Solution

Introduction

- → In Internet of Things (IoT), ubiquitous things are associated with cyber, physical, and social considerations
- → Security and privacy issues become particularly more noteworthy. Several open issues in security and privacy should be considered.
- → For example:

  How do we design appropriate security solutions for different applications?

  What advanced security mechanisms are applied in interconnection among mass things?

  How do we maintain a balance between things' security requirements and supporting infrastructures' hardware limitations?

  How do we achieve a trade-off between individual privacy preserving and information sharing?
- → These security-related issues influence future IoT development, making security and privacy critical issues.
- → Several solutions have been presented for IoT security and privacy issues, including security architectures and recommended countermeasures ,specific communication and sensing techniques, cryptographic mechanisms, and practical applications and scenarios

Introduction (Contd.)

→ The security studies can be categorized into three aspects: system security, network security, and application security.

- System security mainly considers the whole system to identify the security requirements and challenges, to design security frameworks, and to provide recommended security measures.
- Network security focuses on wireless and wired communication networks (e.g., radio frequency identification [RFID], wireless sensor networks [WSNs], and Internet Protocol [IP] network) to design key distribution algorithms, authentication protocols, advanced signature algorithms, and access control mechanisms.
- Application security serves applications (e.g., intelligent transportation and smart grid) and addresses practical problems to satisfy particular scenario requirements

→ In IoT, security and privacy are important to ensure reliable interactions in the physical world and cyber world

Security Challenges in U2IoT

Security Requirements

→ There are four main security requirements in IoT, including CIA triad (Data Confidentiality, Data Integrity, and Data Availability); Authority; Nonrepudiation; and Privacy Preservation.

CIA Triad

- The CIA triad refers to the basic security requirements:

  Confidentiality - Protect data from unauthorized disclosure.

  Integrity - Ensure correctness or accuracy of data.

  Availability - Ensure that there is no denial of authorized access to network elements, information flow, services, and applications.

→ Cryptographic algorithms should be designed to achieve such a CIA triad in the heterogeneous network's infrastructure.

Security Challenges in U2IoT

→ Additional security requirements should also be considered:

- Forward and backward un-linkability - Ensure the interrogations during prior and later sessions of un-linkability, and ubiquitous things cannot be correlated with their corresponding physical, cyber, and social considerations.
- Dynamic session freshness - Applies session freshness mechanisms into the data integrity check to achieve dynamic sessions.
- Self-identification and non-self-identification - Ensure that an authorized self object/entity can access the network resources and services and eliminate any non self object/entity.

Security Challenges in U2IoT

Authority

→ Authority refers to authentication and authorization.

→ The former ensures that only legal things can access network resources and excludes any illegal object/entity from the networks.

→ The latter realizes classified access control among legal things.

→ Meanwhile, additional mechanisms are also considered in U2IoT.

- Intelligent access control -Uses heterogeneous authentication and identification for access control on legal information interoperation.
- Compatible certificate authority - Authenticates object/ entity and grant authority to access system resources.
- Hierarchical authentication - Establishes hierarchical authentication, individual/ group authentication, and source/ terminal authentication.

Security Challenges in U2IoT

Nonrepudiation

→ Nonrepudiation is traditionally defined as providing available proofs to prevent any object/ entity from denying a performed particular behavior/action related to the exchanged messages (Nonrepudiation provides proof of the origin, authenticity and integrity of data) or Non-repudiation refers to the process of ensuring that a message or transaction cannot be denied or rejected by the sender after it has been sent.

→ To ensure the availability of evidence that can be presented by a trusted third party (TTP), and to prove that an object/entity's behavior or action has occurred before.

→ Moreover, social factors are attached to an object/ entity's identity, which are applied for compatible social computing and behavior/action supervision.

Security Challenges in U2IoT

Privacy Preservation

- Privacy refers to individual sensitive information, which may be derived from the observation of network activities and should be protected with the privacy-utility trade-offs.
- In IoT, privacy preservation has additional considerations:
  - Transparency - Lets a user (individual user and group user) know which object/ entity contains the related data, when and where the object/ entity has used the data, and how the object/entity realizes the specific function.
  - Traceability - Lets a user know whether the network and service information have ever connected.

Security Attacks

→ In U2IoT, malicious threats during an interaction are classified into four attack categories: gathering, imitation, blocking, and privacy disclosure.

→ Therefore, the sensor-actuator layer and network layer directly suffer from the gathering, imitation, and blocking attacks, and the application layer mainly confronts the imitation, blocking, and privacy disclosure attacks.

→ In the service integration layer, national management layer, and international coordinator layer, attacks like those in the application layer also suffer.

Security Attacks (Contd.)

Gathering Attack

→ Gathering refers to the data collection–related attacks, including skimming, tempering, eavesdropping, and traffic analysis.

- **Skimming** is an unauthorized access of a quick reading on a target (e.g., RFID tag), and the target's sensitive data are directly read without obtaining authority.
- **Tampering** is an unauthorized data modification or deletion to achieve deliberate data destruction and corruption.
- **Eavesdropping** is unauthorized listening and intercepting via the communication channels of an authorized transmission to record the exchanged data among legal things.
- **Traffic analysis** detects or monitors the exchanged data packets and communication stream, and deduces information from the communication patterns

Security Attacks (Contd.)

Imitation Attack

→ Imitation refers to the attacks of data/ identity cheating, including spoofing, cloning, replay, and Sybil attack.

- **Spoofing** means that an illegal object/ entity imitates a legal data source to transmit duplicate data, in which the object/ entity may be masked as another object/entity by falsifying data and thereby gaining illegal interests.
- **Cloning** refers to an attacker duplicating a legal object/ entity's valid data, and the obtained data can be rewritten into an equivalent object/entity.
- **Replay** occurs when a valid data transmission is intercepted during the former deliveries, then is repeated or delayed by the originator or another object/entity.
- **Sybil attack** represents a reputation system being subverted by creating multiple pseudonyms to forge identities in peer-to-peer (P2P) networks (or) A Sybil attack is a type of security threat in which a single adversary (malicious actor) controls multiple nodes or identities on a network

Security Attacks (Contd.)

Blocking Attack

→ Blocking refers to the active attacks of system or communication channel interferences, including denial of service (DoS), jamming, and malware.

- **DoS** is caused by flooding data streams with false addresses, which interfere in normal communication to overwhelm the system resource, and to render it inoperative.
- **Jamming** interdicts communication channels with an electronic device and disrupts the object/entity’s function by using wireless signals in the same frequency band.
- **Malware** includes computer viruses, worms, Trojan horses, most rootkits, spyware, dishonest adware, and other malicious or unauthorized programs. Additionally, other attacks (e.g., blackhole, sinkhole, and wormhole) are also regarded as malware attacks, which apply malicious nodes to interfere with the the normal routing path selection and communication

Security Attacks (Contd.)

Privacy Disclosure

→ Privacy disclosure refers to sensitive information revelation, including individual privacy disclosure and group privacy disclosure.

- **Individual privacy disclosure** refers to gossip of an individual user’s information, such as locations, interests, and behavior/actions. It correlates sensitive data with the user’s real identity.
- **Group privacy disclosure** includes commercial espionage, in-group/ out-group unauthorized access, and trusted domain disclosure.

Security Attacks (Contd.)

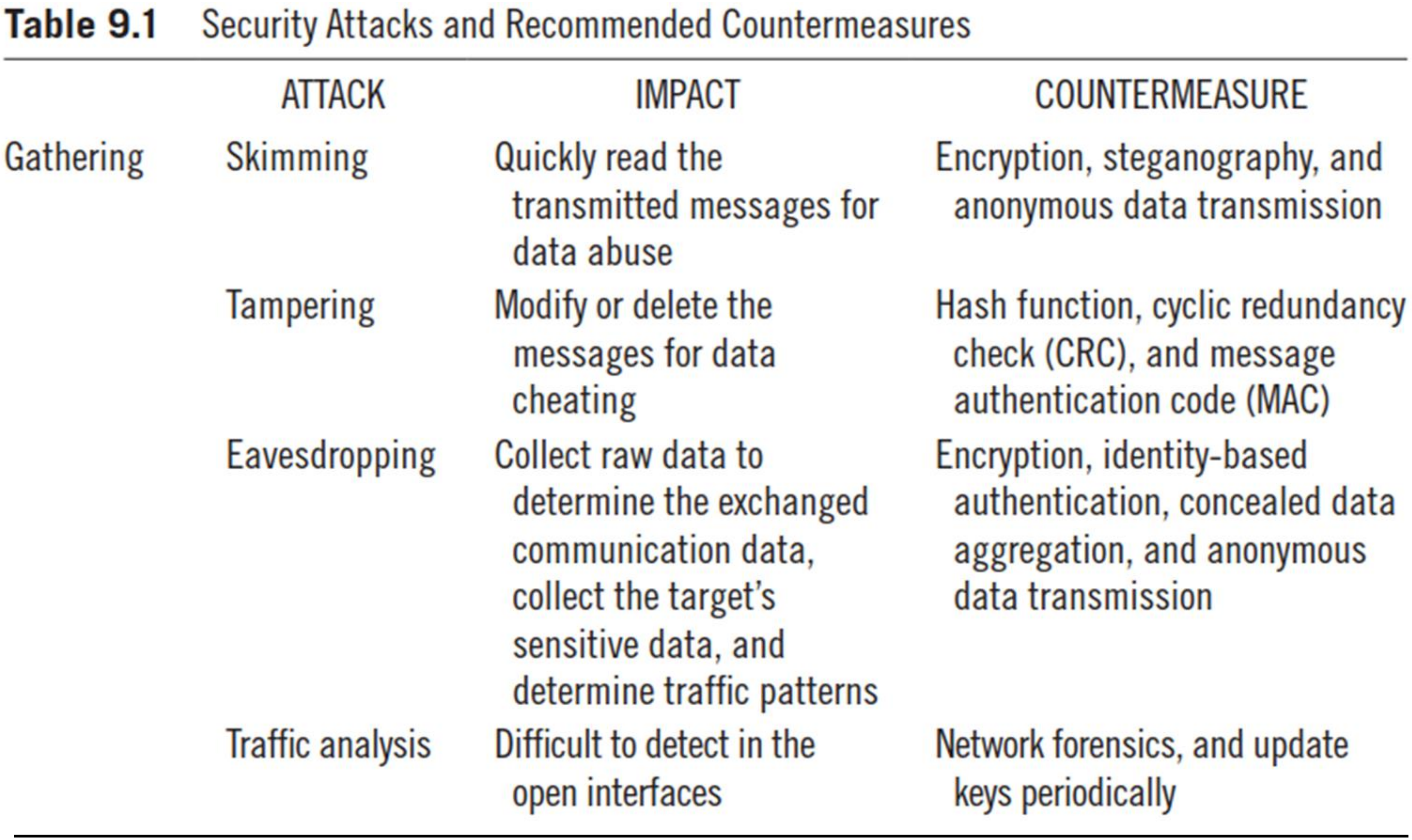


Table 9.1 Security Attacks and Recommended Countermeasures

	ATTACK	IMPACT	COUNTERMEASURE
Gathering	Skimming	Quickly read the transmitted messages for data abuse	Encryption, steganography, and anonymous data transmission
	Tampering	Modify or delete the messages for data cheating	Hash function, cyclic redundancy check (CRC), and message authentication code (MAC)
	Eavesdropping	Collect raw data to determine the exchanged communication data, collect the target's sensitive data, and determine traffic patterns	Encryption, identity-based authentication, concealed data aggregation, and anonymous data transmission
	Traffic analysis	Difficult to detect in the open interfaces	Network forensics, and update keys periodically

Security Attacks (Contd.)

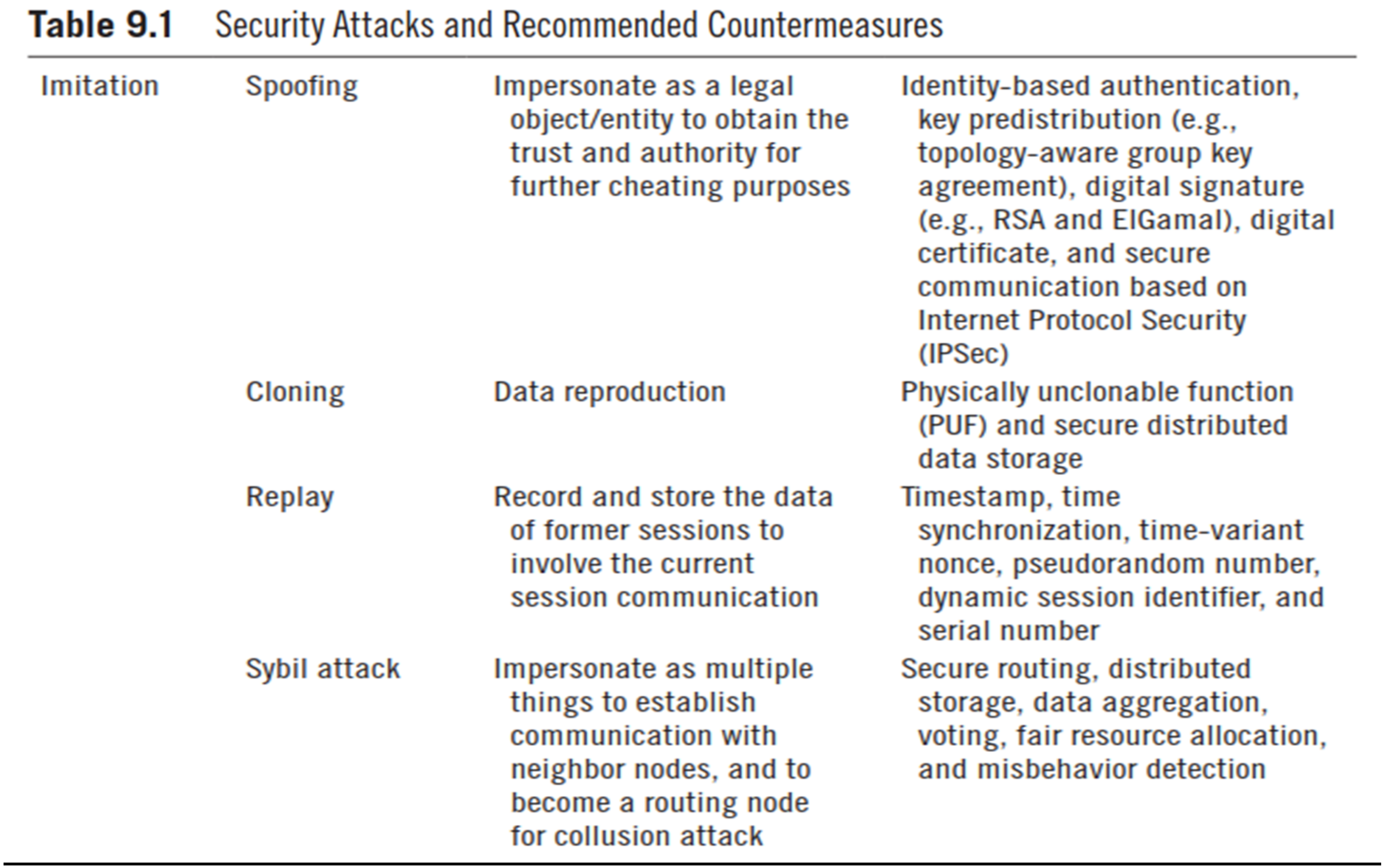


Table 9.1 Security Attacks and Recommended Countermeasures

Imitation	Spoofing	Impersonate as a legal object/entity to obtain the trust and authority for further cheating purposes	Identity-based authentication, key predistribution (e.g., topology-aware group key agreement), digital signature (e.g., RSA and ElGamal), digital certificate, and secure communication based on Internet Protocol Security (IPSec)
	Cloning	Data reproduction	Physically unclonable function (PUF) and secure distributed data storage
	Replay	Record and store the data of former sessions to involve the current session communication	Timestamp, time synchronization, time-variant nonce, pseudorandom number, dynamic session identifier, and serial number
	Sybil attack	Impersonate as multiple things to establish communication with neighbor nodes, and to become a routing node for collusion attack	Secure routing, distributed storage, data aggregation, voting, fair resource allocation, and misbehavior detection

Security Attacks (Contd.)

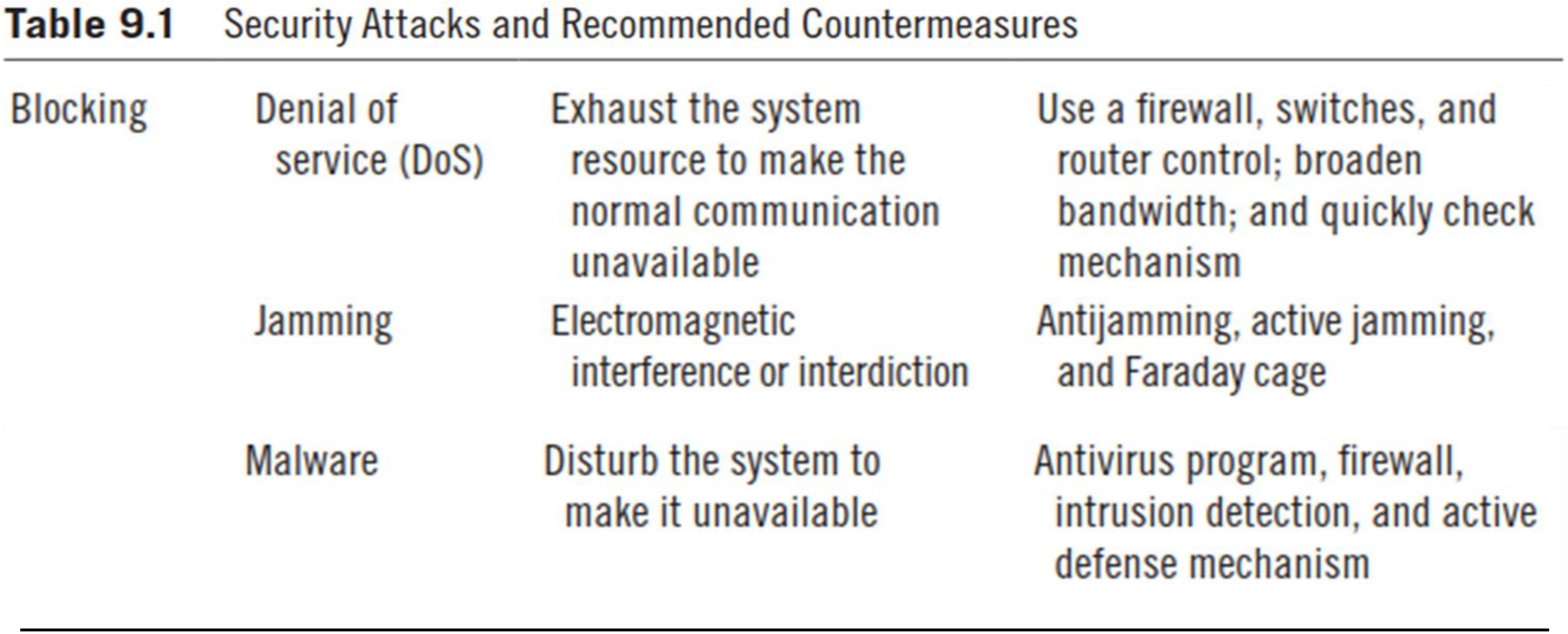


Table 9.1 Security Attacks and Recommended Countermeasures

Blocking	Denial of service (DoS)	Exhaust the system resource to make the normal communication unavailable	Use a firewall, switches, and router control; broaden bandwidth; and quickly check mechanism
	Jamming	Electromagnetic interference or interdiction	Antijamming, active jamming, and Faraday cage
	Malware	Disturb the system to make it unavailable	Antivirus program, firewall, intrusion detection, and active defense mechanism

Security Attacks (Contd.)

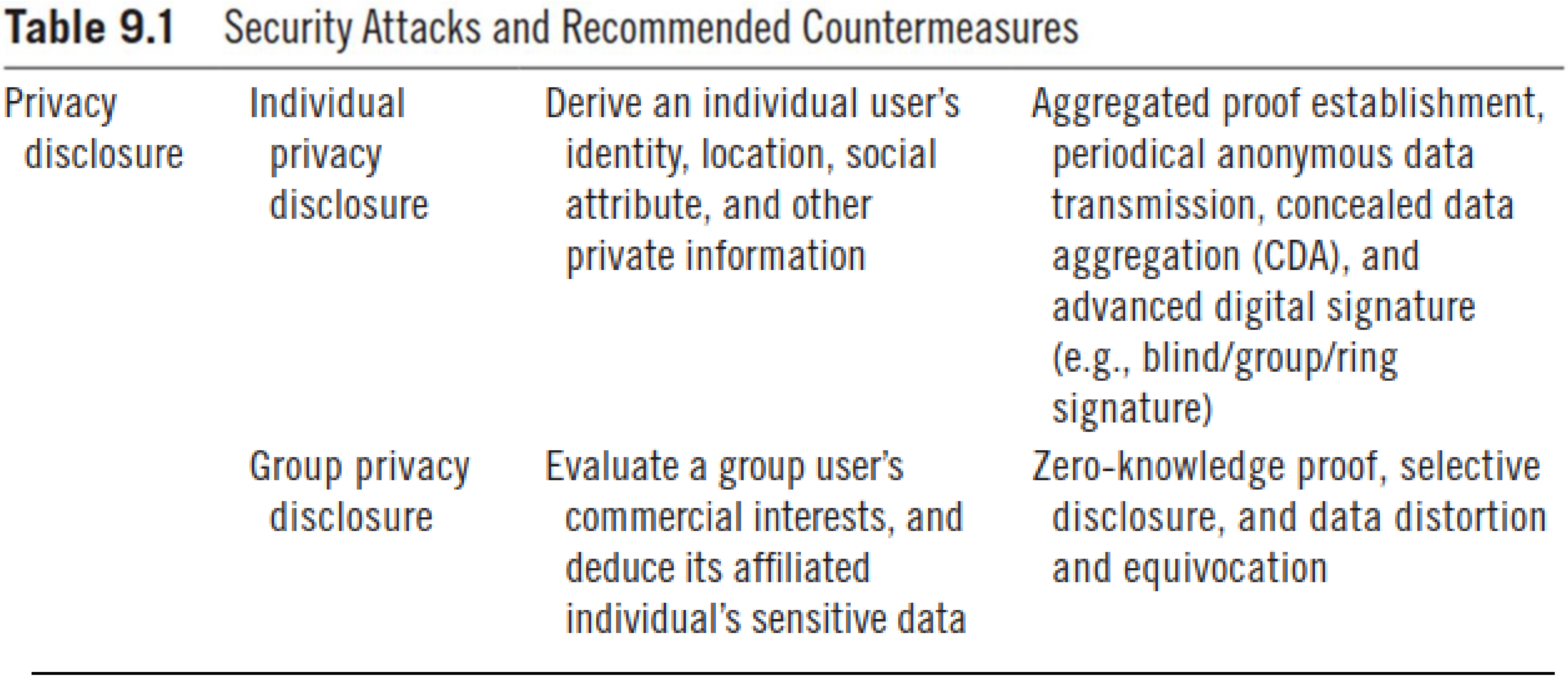


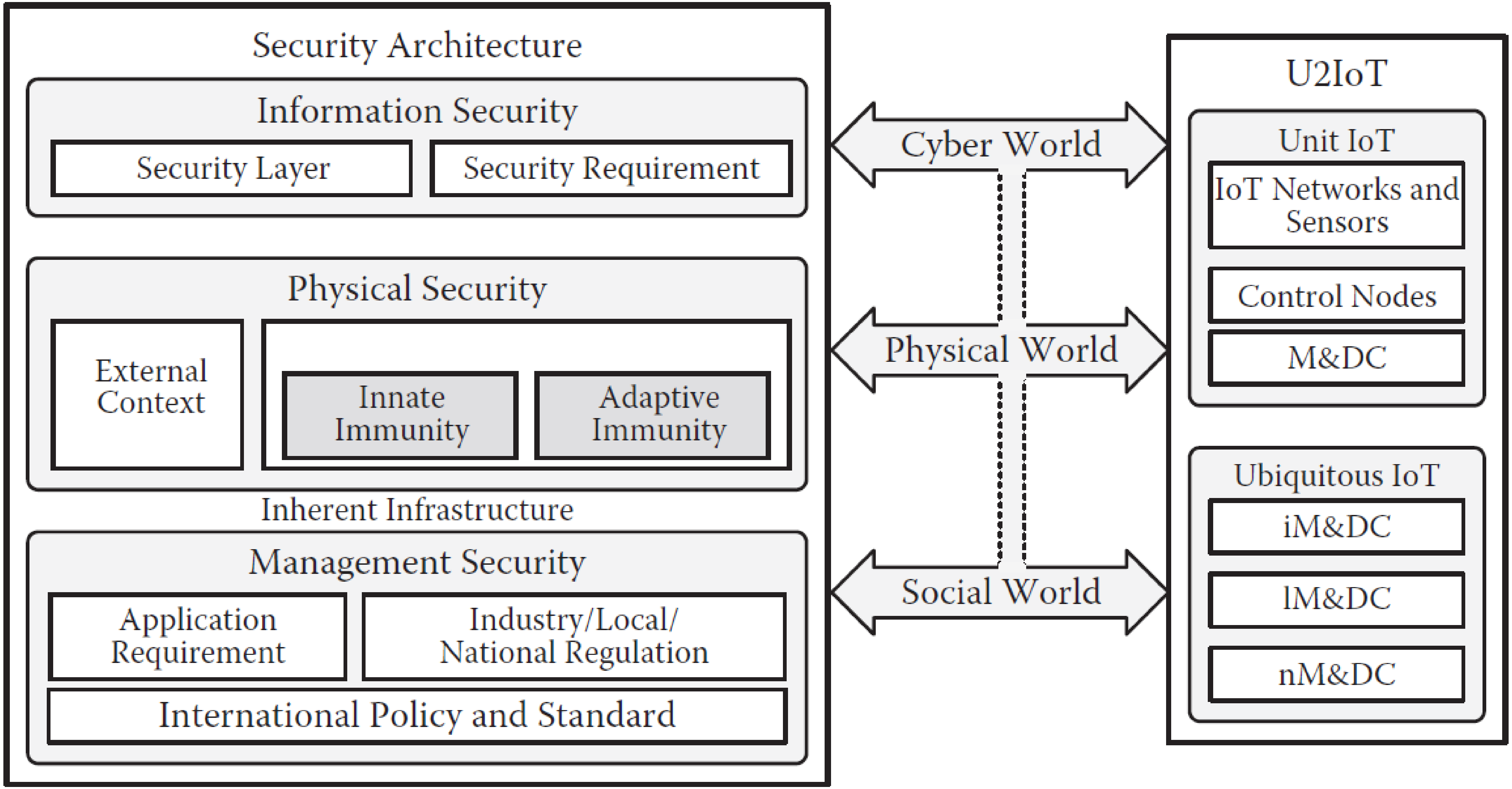
Table 9.1 Security Attacks and Recommended Countermeasures

Privacy disclosure	Individual privacy disclosure	Derive an individual user's identity, location, social attribute, and other private information	Aggregated proof establishment, periodical anonymous data transmission, concealed data aggregation (CDA), and advanced digital signature (e.g., blind/group/ring signature)
	Group privacy disclosure	Evaluate a group user's commercial interests, and deduce its affiliated individual's sensitive data	Zero-knowledge proof, selective disclosure, and data distortion and equivocation

The Security Framework for U2IoT

- A systematic security framework that integrates the awareness and interactivity of the cyber world, physical world, and social world is proposed for U2IoT, as shown in Figure.
- The security framework considers the aspects of information, physical, and management, and realizes the unison of the cyber world, physical world, and social world to address the security and privacy issues in three perspectives
- Information security mainly considers basic and advanced security/privacy issues in the cyber world.
- Awareness of information data is interpreted and represented by things and authentication algorithms, security protocols; interaction functions are also included for intelligent information interactions.

The Security Framework for U2IoT (Contd.)



The Security Framework for U2IoT (Contd.)

- ***Physical security -*** including external context and inherent infrastructure, is inspired by artificial immunity, and ensures that things should be adaptable to dynamic semantic contexts with innate and adaptive immunities against malicious attacks. It relates to environmental monitoring, motion detection, and perimeter control. Artificial immunity is applied to resist passive attacks (e.g., eavesdropping) and active attacks (e.g., spoofing and replay).
- ***Management security -*** provides the recommended strategies for hierarchical classified scenes with rationality and compatibility, including the recommended application requirements; local, industry, or national regulations; and international policy/standards to guide activities and events in human society.
- ***Information security -*** protects both raw data and contextualized information, in which intelligence and compatibility should be considered.
- ***Intelligence -*** that an object/ entity should own the capabilities, including self-learning, self-adapting, and self-reasoning, to adapt itself to dynamic semantic contexts. In nondeterministic channels and open interfaces, virtual intelligent things should be autonomously interconnected in U2IoT. Intelligence makes objects/entities have strong efficacies to adapt dynamic environments, including cyber interactions, social connections, and human participation.

The Security Framework for U2IoT (Contd.)

- ***Compatibility*** - that an object/entity has appropriate interconnection and interoperability mechanisms to adapt to heterogeneous data formats, interfaces, channels, and networks in U2IoT. The supplemental requirements address advanced criteria for information interaction. Meanwhile, compatibility can be promoted to scalability, expansibility, and modularity among the multi-context-based heterogeneous things.
  - The two above-mentioned requirements are jointly applied for information security:
    - To ensure diverse things to own artificial intelligence and autonomous security control against the strong attackers, and
    - To ensure heterogeneous things, networks, and applications to establish reliable interconnection without compromising any communication data and individual privacy.

The Security Framework for U2IoT (Contd.)

Physical Security

→ Physical security is denoted in the external context and inherent infrastructure, in which a human-like security-immune safeguard is implemented.

→ Simple context and complex context are specified by Wang et al. [16], in which the former determines the basic identity, location, and object/entity status by a single parameter, and the latter refers to geographical structures, traceability information, and environment. Both contexts are refined to support creating, debugging, and integrating applications in ubiquitous IoT, and providing a controlled interface for unit IoTs.

→ In U2IoT, the borders of the external context merge—even vanish—and the obscure contexts spanning from an object/ entity, or an environment to social relationships, should support the hierarchical applications. The intrusion detection algorithm is particularly significant for acquiring context information for monitoring sensors, discovering control node breaches, and other potential vulnerabilities.

→ Inherent infrastructure is an artificial immune security system. Computational intelligence is applied to analyze the inherent infrastructure, which belongs to a sensor-based system inspired by principles and processes of the natural immune system. Typical algorithms (e.g., clonal selection, negative selection, and immune network) exploit the immune system's features (e.g., detection, learning capacity, and memory) to constitute innate immunity and adaptive immunity.

The Security Framework for U2IoT (Contd.)

Physical Security

→ Physical security is denoted in the external context and inherent infrastructure, in which a human-like security-immune safeguard is implemented.

→ Simple context and complex context are specified by Wang et al. [16], in which the former determines the basic identity, location, and object/entity status by a single parameter, and the latter refers to geographical structures, traceability information, and environment. Both contexts are refined to support creating, debugging, and integrating applications in ubiquitous IoT, and providing a controlled interface for unit IoTs.

→ In U2IoT, the borders of the external context merge—even vanish—and the obscure contexts spanning from an object/ entity, or an environment to social relationships, should support the hierarchical applications. The intrusion detection algorithm is particularly significant for acquiring context information for monitoring sensors, discovering control node breaches, and other potential vulnerabilities.

→ Inherent infrastructure is an artificial immune security system. Computational intelligence is applied to analyze the inherent infrastructure, which belongs to a sensor-based system inspired by principles and processes of the natural immune system. Typical algorithms (e.g., clonal selection, negative selection, and immune network) exploit the immune system’s features (e.g., detection, learning capacity, and memory) to constitute innate immunity and adaptive immunity.

The Security Framework for U2IoT (Contd.)

Physical Security

→ Physical security issues such as intrusion detection, adaptive disposition, context-driven feedback, and error recovery can be addressed based on the following immunity-inspired mechanisms:

- Innate immunity
  - Innate immunity provides basic defenses against external invasions in a real-time environment, and is triggered by the intelligent pattern recognition mechanisms upon identifying abnormal or malevolent attacks.
  - Costimulation signals are transmitted to distributed control nodes via unit IoT, and then reactions of rejection are performed by management centers.
  - During defense operations, activation thresholds are defined to ensure detection optimization, and fuzzy diagnosis can also be applied for imperfect detection.
  - Note that the innate immune defense is nonspecific, which means that U2IoT responds to the various attacks in a general scheme.
  - Such a system cannot afford long-lasting immunity against a certain attack.
  - The innate immune system is dominant to confront the dynamic contexts and continuously refreshing threats.

The Security Framework for U2IoT (Contd.)

Physical Security

→ Physical security issues such as intrusion detection, adaptive disposition, context-driven feedback, and error recovery can be addressed based on the following immunity-inspired mechanisms:

- Adaptive immunity
  - Adaptive immunity refers to acquired resistance, where an attack is marked as a specific signature.
  - Selective response requires recognizing a nonself object/entity during an attack prototype presentation.
  - If U2IoT has been infected by the same or similar invasion, a specific memory module would be aroused to eliminate damage by generating an improved response to recover the system into a secure state.
  - Adaptive immunity executes fuzzy diagnosis to variations of the same former attack, and optimal stimulation such as subsidiary vaccination is available by updating each management and data center’s (M&DC) profile database.

→ According to the innate and adaptive immunities , there are three main features that can also be considered in IoT physical security.

The Security Framework for U2IoT (Contd.)

Physical Security

→ **Multithreaded and hybrid configuration**

- U2IoT may apply multithreaded security algorithms to the parallel network architecture that comprises a diverse set of components.
- The components are organized in hybrid mode, in which both centralized and distributed configurations are included.
- For unit IoT, the allocation of sensing and query processing is performed by M&DC.
- Industrial IoTs and local IoTs are relatively independent, which commonly construct national IoT.
- In U2IoT, such multithreaded and hybrid configurations are present throughout all the networks, sensors-actuators, and M&DCs.

→ **Multilayered and autonomous organization**

- There is no single security mechanism that offers complete immunity.
- Therefore, multilayered protection should operate independently for enhanced safeguards.
- During the layered organization, U2IoT autonomously makes decisions by detecting potential attacks and proposing feasible solutions based on artificial immune algorithms

The Security Framework for U2IoT (Contd.)

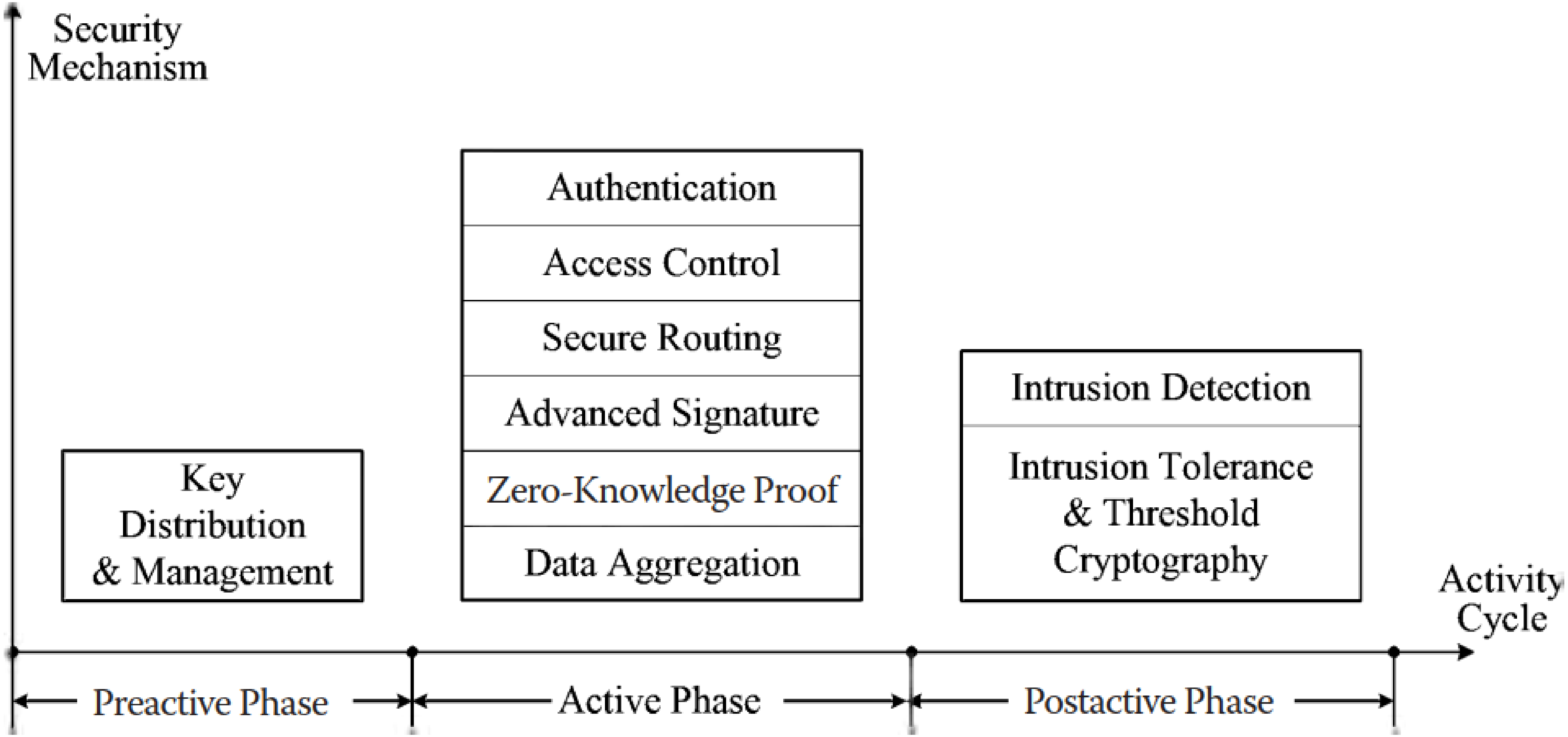
Physical Security

→ **Heterogeneity**

- U2IoT should be accessible by a large number of heterogeneous things with different networks, channels, interfaces, and hardware/software capabilities.
- Such heterogeneity of things adds complexity to its security situations, which allows for a certain attack to simultaneously act on multiple things in different IoTs, but the attack cannot act on all of the involved IoTs.
- Immune protection ensures that the entire heterogeneous components cannot be corrupted due to the same attacker.

Entity Activity Cycle–Based Security Solution

- For security and privacy in IoT, entity-based cyber security is an important aspect. In order to address security and privacy issues in future IoT, an entity activity cycle–based security solution is established to achieve security protection and privacy preservation, as shown in Figure



Entity Activity Cycle–Based Security Solution

Preactive Phase

- Key distribution and management is a fundamental issue in the preactive phase.
- The symmetric key management and distribution technique is a basic approach for communication, in which a preinstalled symmetric key or pairwise shared keys are stored in the memory.
- Meanwhile, an asymmetric key cryptosystem is appropriate to establish a secret key. Identity-based cryptography (IBC) is a typical scheme in WSNs, and the hardness of the bilinear Diffie-Hellman problem (BDHP) and Tate pairing can be applied into key pre-distribution.
- Additionally, a group key agreement scheme can be adopted by multiple things to establish dynamic and deterministic keys, in which bilinear pairing and cryptographic algorithms (e.g., elliptic curve cryptography [ECC], threshold broadcast encryption) can be applied to achieve high efficiency.
- Thus, the shortest path tree (SPT) routing mode and multipath key mode are suitable for the heterogeneous networks and cross-layer communication environments.

Entity Activity Cycle–Based Security Solution

Active Phase

- In the active phase, authentication, access control, securing routing, advanced signature, zero-knowledge proof, and data aggregation are introduced.
- **Authentication**
  - Authentication considers the validity of the interactive things.
  - The traditional authentication modes are mainly based on the shared secrets/keys, entity's identity, and trusted third party (TTP).
  - For authentication operators, ultra-lightweight algorithms such as bitwise logical operators, permutation, and pseudorandom number generators can be applied in the resource-constrained devices (e.g., passive RFID tag); the lightweight algorithms such as hash function, cyclic redundancy check (CRC), and message authentication code (MAC) can be applied to provide enhanced security; and the full-fledged encryption/signature algorithms can be used in the back-end systems.
  - Physical authentication approaches (e.g., physically unclonable function [PUF]) can also be introduced for authentication.

Entity Activity Cycle–Based Security Solution

Active Phase

- In the active phase, authentication, access control, securing routing, advanced signature, zero-knowledge proof, and data aggregation are introduced.
- **Authentication**
  - Authentication considers the validity of the interactive things.
  - The traditional authentication modes are mainly based on the shared secrets/keys, entity’s identity, and trusted third party (TTP).
  - For authentication operators, ultra-lightweight algorithms such as bitwise logical operators, permutation, and pseudorandom number generators can be applied in the resource-constrained devices (e.g., passive RFID tag); the lightweight algorithms such as hash function, cyclic redundancy check (CRC), and message authentication code (MAC) can be applied to provide enhanced security; and the full-fledged encryption/signature algorithms can be used in the back-end systems.
  - Physical authentication approaches (e.g., physically unclonable function [PUF]) can also be introduced for authentication.

Entity Activity Cycle–Based Security Solution

Active Phase

- **Authentication**
  - Moreover, network access authentication is applied to control the things' access in network services; therefore, an IP-based protocol (i.e., protocol for carrying authentication for network access [PANA]) has been standardized by the Internet Engineering Task Force (IETF).
  - Additionally, the authentication mode should fully consider the heterogeneous, mobile, and large-scale networks; therefore, the tiered multicast message authentication and batch authentication mode becomes noteworthy for unit IoTs.

Entity Activity Cycle–Based Security Solution

Active Phase

- **Access Control Access**
  - control refers to the authorization among different things with the classified authorities on a certain system resource.
  - The hybrid access control model can be established according to the access control paradigms (e.g., mandatory access control [MAC], discretionary access control [DAC], role-based access control [RBAC], and attribute-based access control [ABAC]).
  - The space-time characteristic is a key factor so that the temporal role-based access control model should be designed with the geographical location information.
  - Semantic-based and attribute-based models are also feasible for Web services-oriented environments.
  - Along with considering the social factors, a trust-oriented access mode can be established according to the virtualization of the things' profiles.

Entity Activity Cycle–Based Security Solution

Active Phase

- **Secure Routing**
  - Secure routing is represented as dynamic addressing modes, which are traditionally applied along with Internet Protocol Security (IPSec) in computer networks and are also suitable for mobile ad hoc networks (MANETs) and WSNs.
  - The multipath routing and on-demand routing secure protocols can be applied in the heterogeneous sensor networks, and the tree-based, identity-based, and trust-based schemes should be designed to achieve the distributed anonymous data transmission.
- **Advanced Signature**
  - Advanced signature mainly includes blind, group, ring, and identity signature algorithms.
  - Therein, proxy blind signature and partially blind signature schemes can apply bilinear pairings for identity verification, and the Advanced Encryption Standard (AES) cryptosystem can also be introduced into the signature establishment.
  - The blind signature can be introduced into certificateless public key cryptography, and the certificateless pairing-based signature scheme has advantages in the computational cost.

Entity Activity Cycle–Based Security Solution

Active Phase

- **Advanced Signature**
  - The background and foreground knowledge-based offline signature identification can also achieve perfect security unlinkability, and the group/ring signature schemes can combine the anonymous authentication mode to enhance data anonymity.
  - The multisignature and identity-based concurrent signature should consider the privacy preservation by the hybrid aggregation scheme.

Entity Activity Cycle–Based Security Solution

Active Phase

- **Zero-Knowledge Proof**
  - Zero-knowledge proof focuses on the authentication that the interaction between the prover and verifier does not reveal any sensitive information, and both interactive and noninteractive modes are included during the verification.
  - Thus, ECC and blind watermark cryptosystems can be used jointly to achieve zero-knowledge identity verification in the resource-constrained applications.
  - Note that Sigma Protocol with different composition modes (e.g., parallel, EQ, OR, AND) can be applied to realize aggregated multiple-proof verification.
- **Data Aggregation**
  - Data aggregation is applied to achieve privacy preservation, and it realizes that the real-time data of an individual user or a group user cannot reveal sensitive information.
  - The original data aggregation is to aggregate multiple sensing data by performing algebraic or statistical functions to establish a data set for transmission, which has vulnerability on the cluster heads.

Entity Activity Cycle–Based Security Solution

Active Phase

- **Data Aggregation**
  - Concealed data aggregation (CDA) is applied to provide privacy homomorphism (PH) encryption with additive homomorphism to achieve enhanced higher security.
  - Additionally, yoking-proofs or grouping-proofs can be regarded as a data aggregation algorithm, which realizes multiple sensing data, which can be aggregated as a group for further authentication.
  - Meanwhile, hierarchical data aggregation can be applied in the in-network and cross-network aggregations, in which homomorphic encryption and advanced signature algorithms can be jointly added into the aggregation to achieve confidentiality and integrity.

Entity Activity Cycle–Based Security Solution

Post-active Phase

- In the post-active phase, intrusion detection, intrusion tolerance, and threshold cryptography are introduced
- **Intrusion Detection**
  - Intrusion detection detects malicious attacks and enables the systems and communications in secure status.
  - For heterogeneous networks, adaptive network intrusion detection systems with hybrid detection algorithms become necessary.
  - Artificial immune algorithms can be applied to achieve self- and nonself-identifications, and artificial neural networks (ANNs) can also be based to identify real-time intrusions.
  - Meanwhile, data mining techniques (e.g., data collection and feature selection) provide efficient assists to enhance unreliable node detection.

Entity Activity Cycle–Based Security Solution

Post-active Phase

- **Intrusion Tolerance and Threshold Cryptography**
  - Intrusion tolerance refers to secret sharing, and distributes a secret among multiple things, in which each object/entity is allocated a share of the secret.
  - The intrusion tolerance and threshold cryptography realize that multiple things collectively participate in secret management, and even in the case that an object/entity is temporarily inactive or perennially unavailable, other legal things can also perform the normal interaction.
  - Usually, the two mechanisms are used along with other cryptographic algorithms.
  - For example, ECC can be introduced into the secret sharing scheme and threshold signature scheme, a dynamic group key agreement scheme can apply threshold secret sharing to achieve key distribution among multiple things, and a hierarchical secret sharing scheme can be designed according to the hybrid access structures (e.g., multilevel, compartmented, multipartite).

Entity Activity Cycle–Based Security Solution

Post-active Phase

- **Intrusion Tolerance and Threshold Cryptography**
  - Furthermore, fragmentation redundancy scattering (FRS) to harden the tolerance resilience, and segmentation can also be introduced into the overlay secret space for distributed shared memory.
  - Dependable intrusion tolerance (DIT) and hierarchical intrusion tolerance (HIT) should be established for detection-triggered unit IoTs.

Thank you