IoT security: Review, blockchain solutions, and open challenges

Khan, Minhaj Ahmad, and Khaled Salah. *Future Generation Computer Systems* 82 (2018): 395-411.

SeoulTech Cryptography & Information Security Lab.

Byoungjin Seok
2019-03-19

Contents

1 Introduction

2 IoT architecture & Security Challenges

- IoT protocols and standards
- Security requirements for IoT

3 Categorization of security issues

- Low-level security issues
- Intermediate-level security issues
- High-level security issues

4 Security solutions for IoT

- Low-level security solutions
- Intermediate-level security solutions
- High-level security solutions

Contents

5 Blockchain solutions for IoT security

- Background for understanding a blockchain
- Potential blockchain solutions

6 Open challenges and future research directions

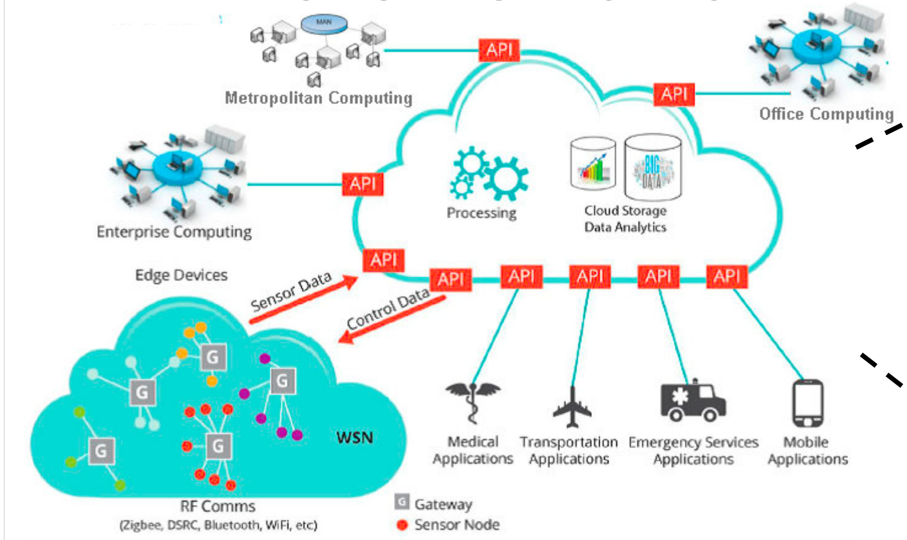
- Resource limitations
- Heterogenous devices
- Interoperability of security protocols
- Single points of failure
- Hardware/firmware vulnerabilities
- Trusted updates and management
- Blockchain vulnerabilities

7 Conclusion

Internet of Things (IoT)

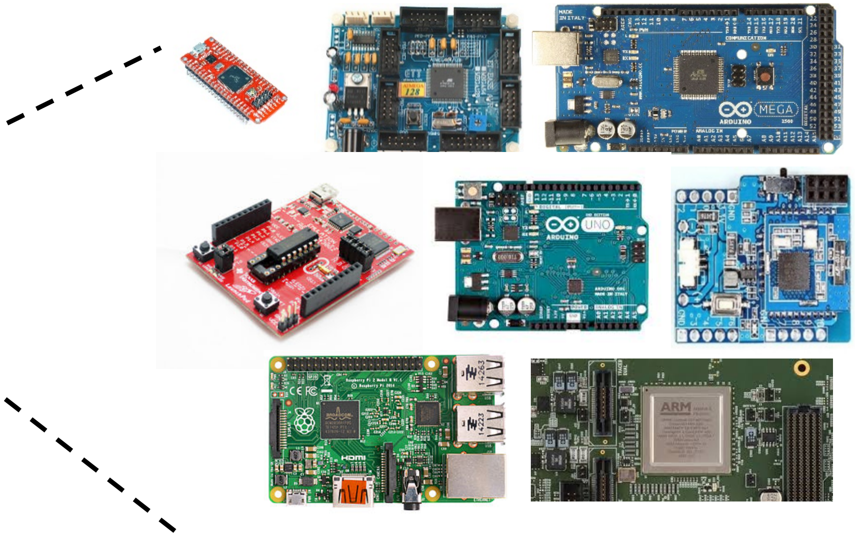
- IoT represents a network where "things" or embedded devices having sensors are interconnected through a private or a public network. And usually these devices are resource-constrained.
- IoT paradigm represents a collection of interconnected networks, and heterogeneous devices, it inherits the conventional security issues related to the computer networks.
- However, the constrained resources pose further challenges to IoT security since the small devices or things containing sensors have limited power and memory. This is the main reason why we can not adopt the existing security solutions to the IoT network.

Overview of IoT



Ref: https://www.researchgate.net/figure/Overview-of-communications-in-the-IoT-network_fig1_329133241

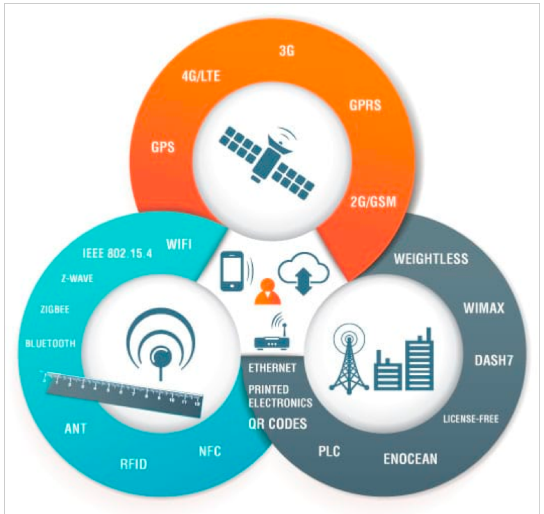
Embedded devices



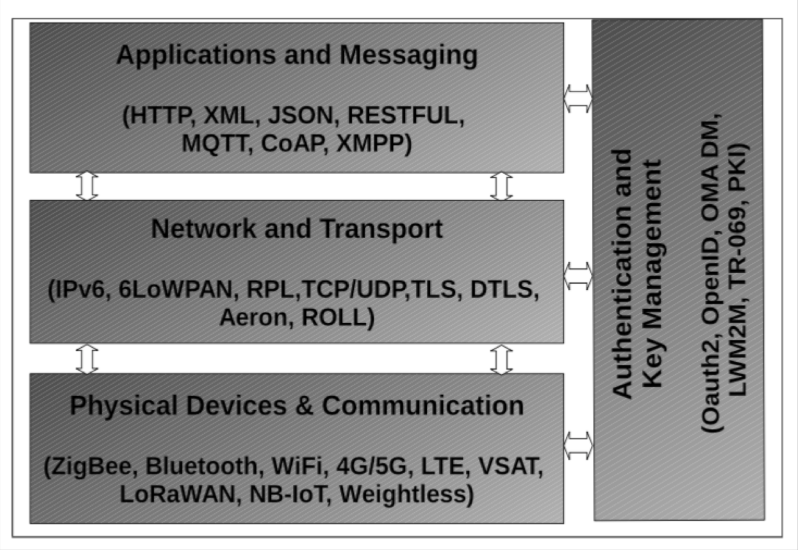
Main contributions of this paper

- Analysis of security threats and their mapping to possible solutions for IoT.
- Taxonomy and categorization of IoT security issues with respect to its layers, and the countermeasures used to address these issues.
- Discussion of basic characteristics of the blockchain based security solutions and analysis of their effectiveness for securing IoT.
- Future directions highlighting possible solutions for open IoT security problems.

Common IoT standard and protocol



Ref: https://www.postscapes.com/internet-of-things-technologies/



Applications and Messaging

(HTTP, XML, JSON, RESTFUL, MQTT, CoAP, XMPP)

Network and Transport

(IPv6, 6LoWPAN, RPL,TCP/UDP,TLS, DTLS, Aeron, ROLL)

Physical Devices & Communication

(ZigBee, Bluetooth, WiFi, 4G/5G, LTE, VSAT, LoRaWAN, NB-IoT, Weightless)

Authentication and Key Management

(Oauth2, OpenID, OMA DM, LWM2M, TR-069, PKI)

There are many IoT standard and protocol.
In this paper, they categorized communication protocols in point of IoT architecture as follows:

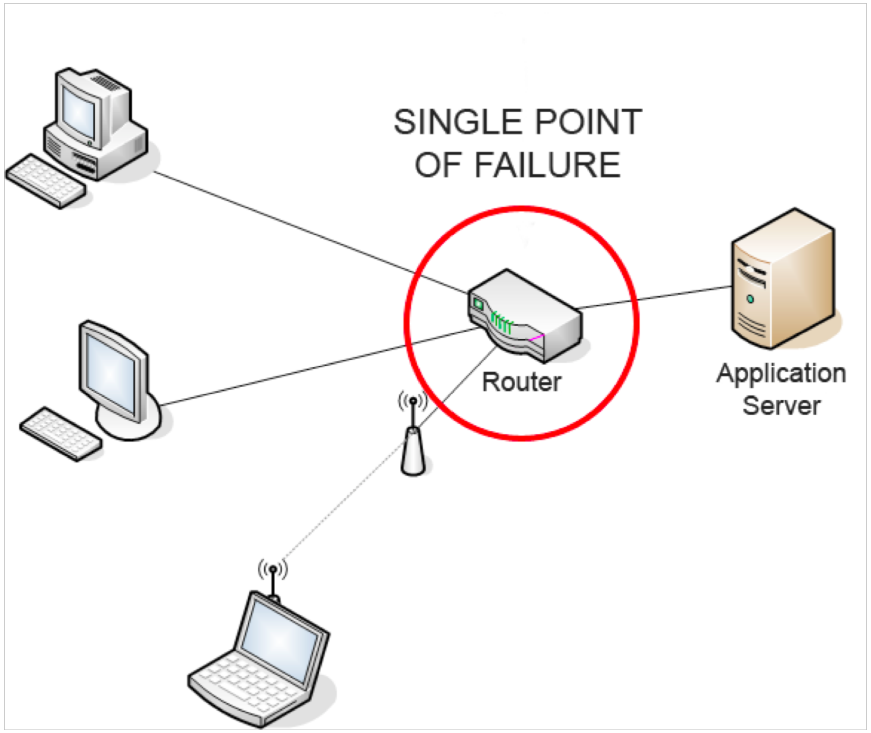
- Applications and Messaging = High-level
  - ✓ applications executing on IoT
- Network and Transport = Intermediate-level
  - ✓ mainly concerned with the communication, routing and session management
- Physical Devices & Communication = Low-level
  - ✓ hardware level

Security requirements for IoT

- Data privacy, confidentiality and integrity
  - As IoT data travels through multiple hops in a network, a proper encryption mechanism is required to ensure the confidentiality of data.
- Authentication, authorization and accounting
  - The diversity of authentication mechanisms for IoT exists mainly due to the diverse heterogeneous underlying architectures and environments which support IoT devices.
  - These environment pose a challenge for defining standard global protocol for authentication in IoT
- Availability of services
  - The attacks on IoT devices may hinder this provision of services through the conventional denial-of-service attacks
- Energy efficiency
  - The IoT devices are typically resource-constrained and are characterized with low power and less storage.
  - The attacks on IoT architectures may result in an increase in energy consumption.

Security requirements for IoT(Con’t)

- Single points of failure
  - A continuous growth of heterogeneous networks for the IoT-based infrastructure may expose a large number of single-points-of-failure.
  - It necessitates the development of a tamper-proof environment for a large number of IoT devices as well as to provide alternative mechanism for implementation of a fault tolerant network.



Ref: https://en.wikipedia.org/wiki/Single_point_of_failure

Three levels of IoT security issues

Low-level security issues

- Jamming adversaries
- Insecure initialization
- Low-level Sybil and spoofing attacks
- Insecure physical interface
- Sleep deprivation attack

physical and data link layers of communication and hardware level

Intermediate-level security issues

- Replay and duplication attacks due to fragmentation
- Insecure neighbor discovery
- Buffer reservation attack
- RPL routing attack
- Sinkhole and wormhole attacks
- Sybil attacks on intermediate layers
- Authentication and secure communication
- Transport level end-to-end security
- Session establishment and resumption
- Privacy violation on cloud-based IoT

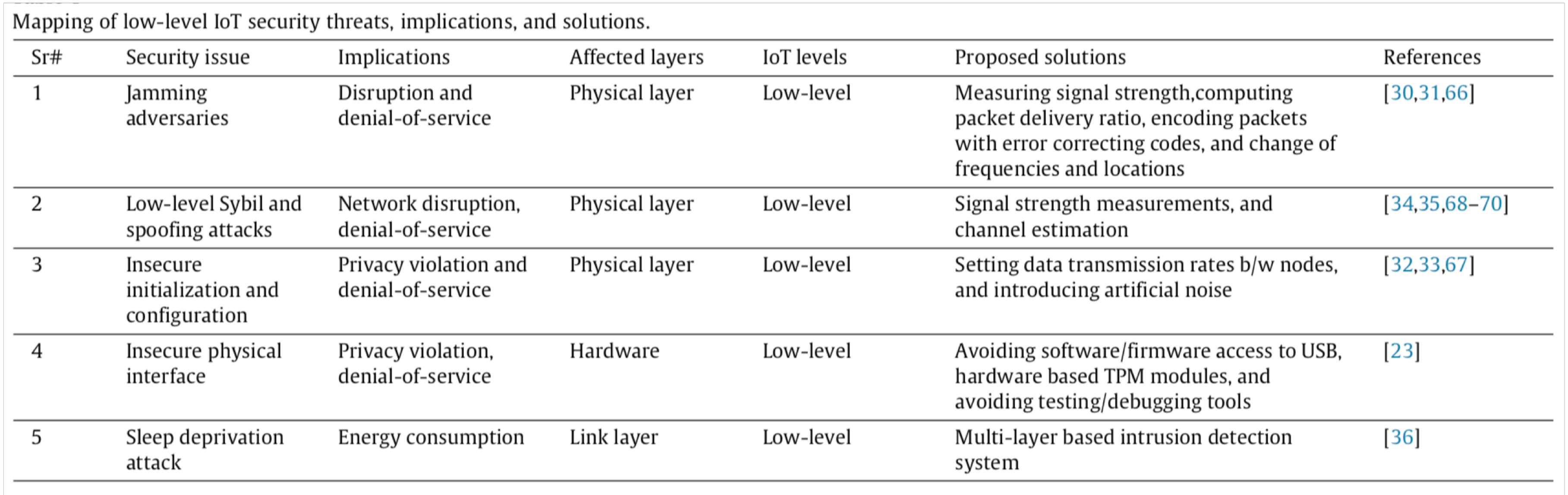
network and transport layers of IoT

High-level security issues

- CoAP security with internet
- Insecure interfaces
- Insecure software/firmware
- Middleware security

Applications executing on IoT

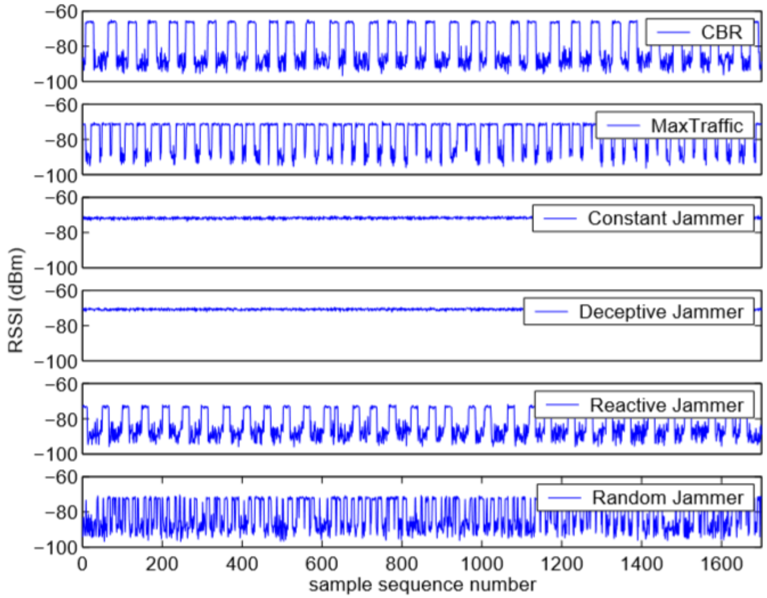
Security solutions for Low-level IoT



Mapping of low-level IoT security threats, implications, and solutions.

Sr#	Security issue	Implications	Affected layers	IoT levels	Proposed solutions	References
1	Jamming adversaries	Disruption and denial-of-service	Physical layer	Low-level	Measuring signal strength,computing packet delivery ratio, encoding packets with error correcting codes, and change of frequencies and locations	[30,31,66]
2	Low-level Sybil and spoofing attacks	Network disruption, denial-of-service	Physical layer	Low-level	Signal strength measurements, and channel estimation	[34,35,68–70]
3	Insecure initialization and configuration	Privacy violation and denial-of-service	Physical layer	Low-level	Setting data transmission rates b/w nodes, and introducing artificial noise	[32,33,67]
4	Insecure physical interface	Privacy violation, denial-of-service	Hardware	Low-level	Avoiding software/firmware access to USB, hardware based TPM modules, and avoiding testing/debugging tools	[23]
5	Sleep deprivation attack	Energy consumption	Link layer	Low-level	Multi-layer based intrusion detection system	[36]

Security solutions for Low-level IoT



RSSI readings as a function of time in different scenarios. RSSI values were sampled every 1msec.

[Jamming adversaries]

- The Jamming attacks on wireless devices in IoT target deterioration of the networks by emitting radio frequency signals without following a specific protocol.
- The radio interference severely impacts the network operations and can affect the sending and receiving of data by legitimate nodes, resulting in malfunctioning or unpredictable behavior of the system.
- Implications : Disruption & Denial-of-Service

[solution]

- The detection of attacks is made possible by measuring the signal strength(statistics)
- Computation of successful packet delivery ratio. (consistency check on signal strength and locations of the nodes.)
- Using cryptographic functions and error correcting codes. (interleaving)
- Change of frequencies and locations.

Security solutions for Low-level IoT(Con’t)

[Low-level Sybil and Spoofing attacks]

- The Sybil attacks in a wireless network are caused by malicious Sybil nodes which use fake identities to degrade the IoT functionality.
- On the physical layer, a Sybil node may use a random forged MAC values for masquerading as a different device while aiming at depletion of network resources.
- Similarly, the spoofing attack is that the attacker masquerades as another node by forging the identity.
- Implications : Network disruption, Denial-of-Service

[solution]

- Signal strength measurements by deploying detector nodes to compute the sender location during message communication.
- Signal strength measurements for MAC address.
- Incorporates channel estimation for detecting Sybil attacks.

Security solutions for Low-level IoT(Con't)

[Insecure initialization and configuration]

- A secure mechanism of initializing and configuring IoT at the physical layer ensures a proper functionality of the entire system without violating privacy and disruption of network services.
- The physical layer communication also need to be secured in order to make it inaccessible to unauthorized receivers.
- Implications : Privacy violation, Denial-of-Service

[solution]

- A minimum data rate is configured between the sending and receiving nodes to ensure absence of eavesdroppers. (analyzed about system parameters)
- Introducing artificial noise in signal

Security solutions for Low-level IoT(Con't)

[Insecure physical interface]

- Several physical factors compound serious threats to proper functioning of devices in IoT.
- The poor physical security software access through physical interfaces, and tools for testing/debugging may be exploited to compromise nodes in the network.
- Implications : Privacy violation, Denial-of-Service

[solution]

- The unnecessary hardware interfaces such as USBs providing access to the device firmware/software must be avoided.
- The testing and debugging tools must be disabled and hardware based mechanism such as Trusted Platform Modules (TPMs) should be incorporated to improve physical security.

Security solutions for Low-level IoT(Con't)

[Sleep deprivation attack]

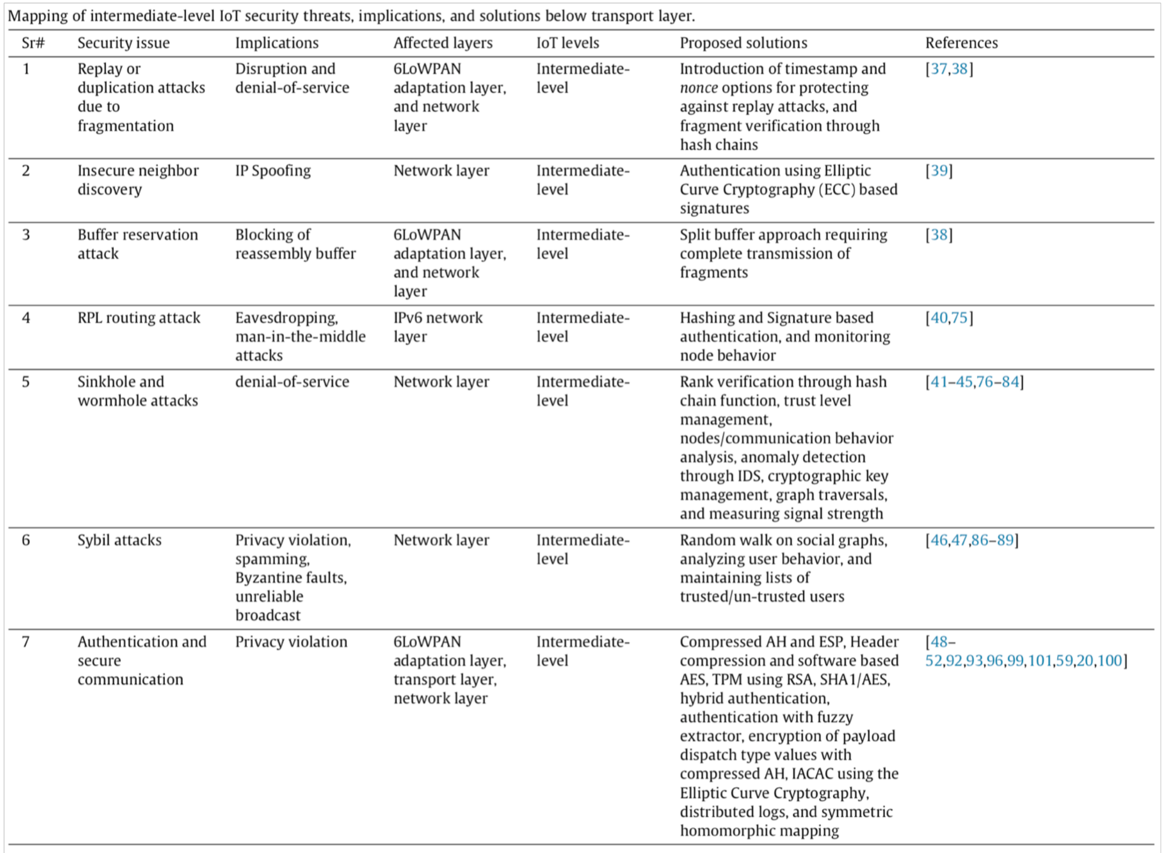
- The energy constrained devices in IoT are vulnerable to "sleep deprivation" attacks by causing the sensor nodes to stay awake.
- It results in depletion of battery when a large number of tasks is set to be executed in the 6LoWPAN(IPv6 over Low-Power Wireless Personal Area Network) environment.
- Implications : Energy consumption

[solution]

- Intrusion detection with a multi-layers model of the wireless sensor network.
- A cluster coordinator contains an extended intrusion detection system together with the leader nodes and sink nodes in upper layers of the wireless sensor network(WSN)

Security solutions for Intermediate-level IoT

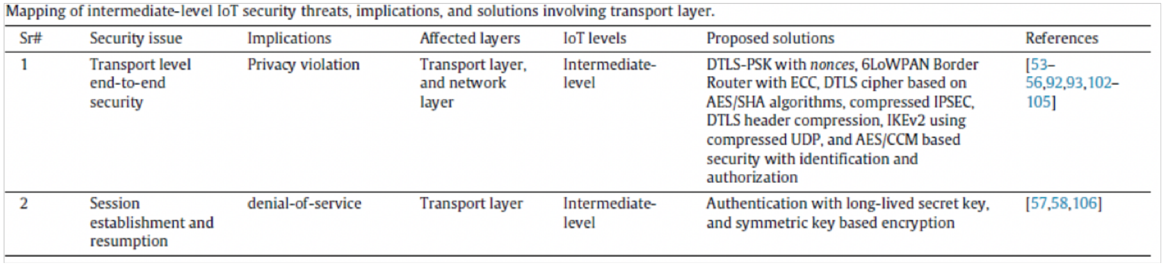
Below transport layer



Mapping of intermediate-level IoT security threats, implications, and solutions below transport layer.

Sr#	Security issue	Implications	Affected layers	IoT levels	Proposed solutions	References
1	Replay or duplication attacks due to fragmentation	Disruption and denial-of-service	6LoWPAN adaptation layer, and network layer	Intermediate-level	Introduction of timestamp and *nonce* options for protecting against replay attacks, and fragment verification through hash chains	[37,38]
2	Insecure neighbor discovery	IP Spoofing	Network layer	Intermediate-level	Authentication using Elliptic Curve Cryptography (ECC) based signatures	[39]
3	Buffer reservation attack	Blocking of reassembly buffer	6LoWPAN adaptation layer, and network layer	Intermediate-level	Split buffer approach requiring complete transmission of fragments	[38]
4	RPL routing attack	Eavesdropping, man-in-the-middle attacks	IPv6 network layer	Intermediate-level	Hashing and Signature based authentication, and monitoring node behavior	[40,75]
5	Sinkhole and wormhole attacks	denial-of-service	Network layer	Intermediate-level	Rank verification through hash chain function, trust level management, nodes/communication behavior analysis, anomaly detection through IDS, cryptographic key management, graph traversals, and measuring signal strength	[41–45,76–84]
6	Sybil attacks	Privacy violation, spamming, Byzantine faults, unreliable broadcast	Network layer	Intermediate-level	Random walk on social graphs, analyzing user behavior, and maintaining lists of trusted/un-trusted users	[46,47,86–89]
7	Authentication and secure communication	Privacy violation	6LoWPAN adaptation layer, transport layer, network layer	Intermediate-level	Compressed AH and ESP, Header compression and software based AES, TPM using RSA, SHA1/AES, hybrid authentication, authentication with fuzzy extractor, encryption of payload dispatch type values with compressed AH, IACAC using the Elliptic Curve Cryptography, distributed logs, and symmetric homomorphic mapping	[48–52,92,93,96,99,101,59,20,100]

Involving transport layer



Mapping of intermediate-level IoT security threats, implications, and solutions involving transport layer.

Sr#	Security issue	Implications	Affected layers	IoT levels	Proposed solutions	References
1	Transport level end-to-end security	Privacy violation	Transport layer, and network layer	Intermediate-level	DTLS-PSK with *nonces*, 6LoWPAN Border Router with ECC, DTLS cipher based on AES/SHA algorithms, compressed IPSEC, DTLS header compression, IKEv2 using compressed UDP, and AES/CCM based security with identification and authorization	[53–56,92,93,102–105]
2	Session establishment and resumption	denial-of-service	Transport layer	Intermediate-level	Authentication with long-lived secret key, and symmetric key based encryption	[57,58,106]

Security solutions for Intermediate-level IoT below transport layer

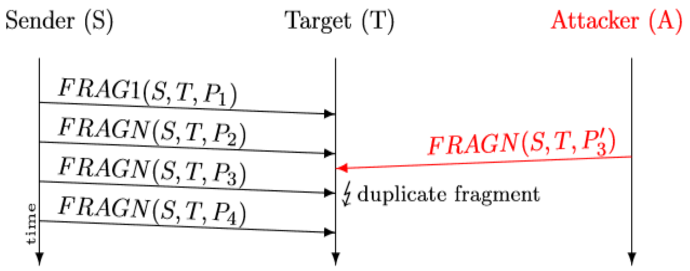


Figure 3: Packet diagram depicting the fragment duplication attack. A target must decide which fragment payload (P_3 or P'_3) to use during reassembly.

[Reply or duplication attack due to fragment]

- A reconstruction of the packet fragment fields at the 6LoWPAN layer may result in depletion of resources, buffer overflows and rebooting of the devices.
- The duplicate fragments sent by malicious nodes affect the packet re-assembly, thereby hindering the processing of other legitimate packets.
- Implications : Disruption, denial-of-service

[solution]

- The 64bit timestamp value in the fragment ensures to eliminate the redundant advertisements and redirects in the network.
- The nonce option ensure that the advertisement is only made to respond to a fresh solicitation.
- Hash chain

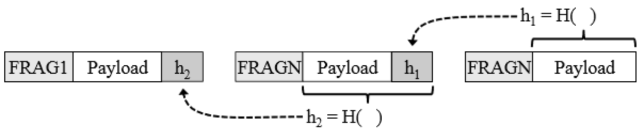
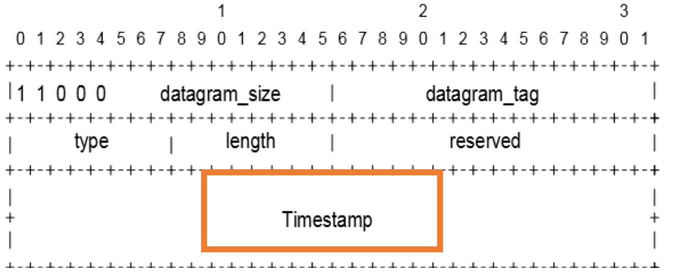
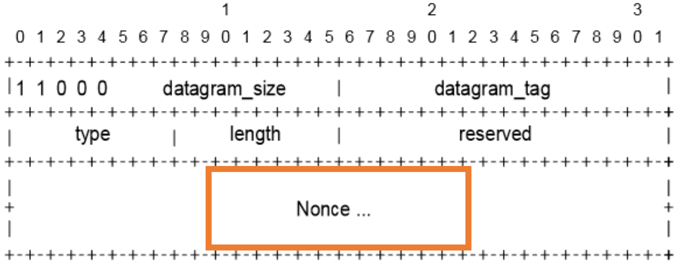


Figure 5: Example of a content chain for a packet consisting of three fragments.



```
                     1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|1 1 0 0 0    datagram_size    |         datagram_tag          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     type      |    length     |           reserved            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                           Timestamp                           +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```



```
                     1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|1 1 0 0 0    datagram_size    |         datagram_tag          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     type      |    length     |           reserved            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                           Nonce ...                           +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Security solutions for Intermediate-level IoT below transport layer(Con’t)

[Insecure neighbor discovery]

- The neighbor discovery phase prior to transmission of data performs different steps including the router discovery and address resolution.
- The usage of neighbor discovery packets without proper verification may have severe implications along with denial-of-service.
- Implications : IP Spoofing

[solution]

- ECC public key signatures are used to identify nodes in the neighbor discovery phase.

Security solutions for Intermediate-level IoT below transport layer(Con't)

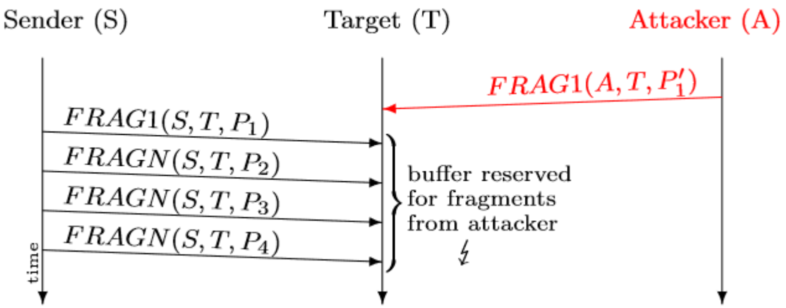


Figure 4: Packet diagram illustrating the buffer reservation attack. After the attack, the reassembly buffer of the target node is occupied by attacker fragments until the reassembly timeout expires.

[Buffer reservation attack]

- As receiving node requires to reserve buffer space for re-assembly of incoming packets, an attacker may exploit it by sending incomplete packets.
- The attack results in denial-of-service as other fragment packets are discarded due to the space occupied by incomplete packets sent by the attacker.
- Implications : Blocking of reassembly buffer

[solution]

- This attack is mitigated through split buffer approach which increases the cost of launching attack by requiring complete fragmented packets to be transmitted in short bursts.
  - Every node is required to compute the percentage of completion of a packet and record the behavior of sending fragments.

Security solutions for Intermediate-level IoT below transport layer(Con't)

[RPL routing attack]

- The IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) is vulnerable to several attacks triggered through compromised nodes existing in the network.
- Implications : Eavesdropping, main-in-the-middle attacks.

[solution]

- Version number and rank authentication uses the hash function, mac function for authenticating version numbers and ranks.
- Monitor node behavior for various parameters including the messages delivered and the end-to-end delay etc.

Security solutions for Intermediate-level IoT below transport layer(Con't)

[Sinkhole and wormhole attacks]

- With the sinkhole attacks, the attacker node responds to the routing requests, thereby making the packets route through the attacker node which can then be used to perform malicious activity on the network.
- The attacks on network may further deteriorate the operations of 6LoWPAN due to wormhole attacks in which a tunnel is created between two nodes so that packets arriving at a node reach other node immediately.
- Implications : denial-of-services.

[solution]

- Rank verification corresponding to a Destination Information Object message, a one-way hash function is used together with a hash chain function.
  - Rank verification ensures that compromised nodes can only lower their rank by 1.
- Trust level management -> trust measurement by monitoring other node's participation
- nodes/communication behavior analysis, anomaly detection through IDS, cryptographic key management, graph traversals, measuring signal strength.

Security solutions for Intermediate-level IoT below transport layer(Con't)

[Sybil attacks]

- The Sybil attacks on network layer use pseudo-identities to mimic multiple unique identities termed as Sybil nodes.
- Implications : Privacy violation, spamming, Byzantine faults

[solution]

- The countermeasures using social graphs make it possible for legitimate nodes to detect Sybil nodes by traversing the graph through random walks or using the community detection algorithms.
- User's behavior regarding activities on the network are analyzed, and subsequently, the users with a fixed pattern of activities are assumed to be Sybil users.
- For mobile networks, the lists of trusted and untrusted users may be maintained to detect Sybil nodes.

Security solutions for Intermediate-level IoT below transport layer(Con't)

[Authentication and secure communication]

- The devices and users in IoT need to be authenticated through key management systems.
- Any loophole in security at network layer or large over-head of securing communication may expose the network to a large number of vulnerabilities.
- IoT must take into account the efficiency as well as the scarcity of other resources.
- Implications : privacy violation

[solution]

- IPSec
    - Compressed formats of Authentication Header (AH) and Encapsulating Security Payload(ESP)
    - Encryption of payload dispatch type values with compressed AH
- Authentication using extracting secret random string from biometrics. (password)
- Use variants of SHA1 and AES
- Trusted Platform Module chips using RSA

Security solutions for Intermediate-level IoT involving transport layer

[Transport level end-to-end security]

- The transport level end-to-end security aims at providing secure mechanism so that the data from the sender node is received by the desired destination node in a reliable manner.
- It requires comprehensive authentication mechanisms which ensure secure message communication in encrypted form without violating privacy while working with minimum overhead.
- Implications : Privacy violation

[solution]

- DTLS
  - DTLS-PSK with nonce(for session key), DTLS cipher based on AES/SHA algorithms, DTLS header compression
- IPsec
  - Compressed IPSEC, IKEv2 using compressed UDP
- 6LoWPAN Border Router with ECC (An Access Control sever is incorporated to support authentication between 6LBR and sensing devices.)
- AES/CCM based security with identification and authorization.

Security solutions for Intermediate-level IoT involving transport layer(Con't)

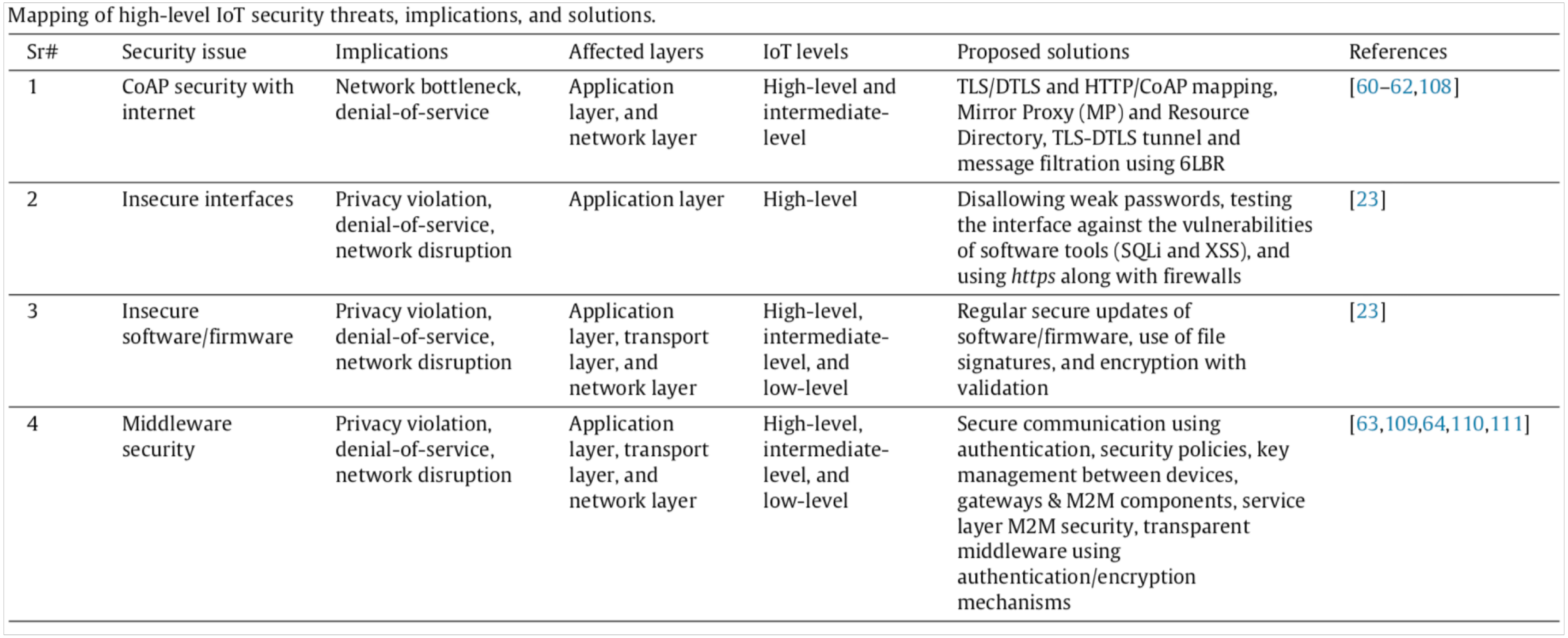
[Session establishment and resumption]

- An attacking node can impersonate the victim node to continue the session between two nodes.
- The communicating nodes may even require re-transmission of messages by altering the sequence numbers.
- Implications : denial-of-service

[solution]

- Initially selects a random number, and perform encryption, and generates a session key which is subsequently used for encryption of another random number.
  - a new session key may be generated without requiring of parameters.
- Having a long-lived secret key which is then used for authentication

Security solutions for High-level IoT



Mapping of high-level IoT security threats, implications, and solutions.

Sr#	Security issue	Implications	Affected layers	IoT levels	Proposed solutions	References
1	CoAP security with internet	Network bottleneck, denial-of-service	Application layer, and network layer	High-level and intermediate-level	TLS/DTLS and HTTP/CoAP mapping, Mirror Proxy (MP) and Resource Directory, TLS-DTLS tunnel and message filtration using 6LBR	[60–62,108]
2	Insecure interfaces	Privacy violation, denial-of-service, network disruption	Application layer	High-level	Disallowing weak passwords, testing the interface against the vulnerabilities of software tools (SQLi and XSS), and using *https* along with firewalls	[23]
3	Insecure software/firmware	Privacy violation, denial-of-service, network disruption	Application layer, transport layer, and network layer	High-level, intermediate-level, and low-level	Regular secure updates of software/firmware, use of file signatures, and encryption with validation	[23]
4	Middleware security	Privacy violation, denial-of-service, network disruption	Application layer, transport layer, and network layer	High-level, intermediate-level, and low-level	Secure communication using authentication, security policies, key management between devices, gateways & M2M components, service layer M2M security, transparent middleware using authentication/encryption mechanisms	[63,109,64,110,111]

Security solutions for High-level IoT

[CoAP security with internet]

- Constrained Application Protocol(CoAP) being a web transfer protocol for constrained device uses DTLS bindings with various security modes to provide end-to-end security.

- Implications : Network bottleneck, denial-of-service

[solution]

- Mapping TLS and DTLS in 6LoWPAN Border Router
- Using public key cryptography.

Security solutions for High-level IoT(Con’t)

[Insecure interfaces]

- For accessing IoT services, the interfaces used through web, mobile, and cloud are vulnerable to different attacks which may severely affect the data privacy.
- Implications : Privacy violation, denial-of-service, network disruption

[solution]

- The security mechanisms include the configurations which discourage weak passwords
- Testing the interface against the well-known vulnerability of software tools(SQLi and XSS)
- The usage of https along with the firewalls.

❖ SQLi : SQL Injection

❖ XSS : cross site scripting

Security solutions for High-level IoT(Con't)

[Insecure software/firmware]

- Various vulnerabilities in IoT include those caused by insecure software/firmware.
- The code with languages such as JSON, XML, SQLi and XSS needs to be tested carefully.
- The software/firmware updates need to be carried out in a secure manner.
- Implication : Privacy violation, denial-of-service, network disruption

[solution]

- The software or firmware installed on the device should be updated regularly through an encrypted transmission mechanism.
- The updated files should be downloaded from a secure sever and these files must be signed and properly validated prior to installation. (use of file signatures and encryption with validation)

Security solutions for High-level IoT(Con’t)

[Middleware security]

- The IoT middleware designed to render communication among heterogeneous entities of the IoT paradigm must be secure enough for provision of services.

- Different interfaces and environments using middleware need to be incorporated to provide secure communication.

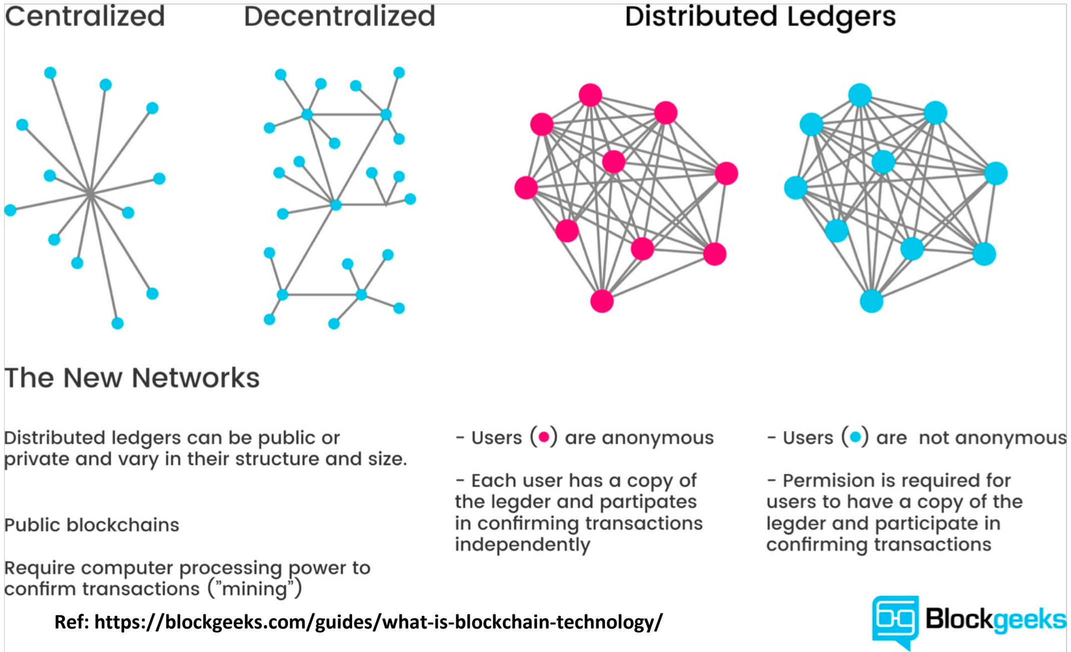
- Implication : Privacy violation, denial-of-service, network disruption

[solution]

- Securing communication using authentication, security policies, key management between devices, gateways&M2M components
- Using standard encryption method
- Using TLS,DTLS session

Background for understanding a blockchain

- In traditional recording method , there are Trusted Third Party (TTP).
- In blockchain technology there is no Trusted Third Party (TTP). everyone record all transaction. and we can trust each other by compare each other's ledger.
- Block is form of recording transaction and chain is way of make blocks.
- Blockchain is fundamentally a decentralized, distributed, shared, and immutable database ledger that stores registry of assets and transactions across a peer-to-peer network



The New Networks

Distributed ledgers can be public or private and vary in their structure and size.

Public blockchains

Require computer processing power to confirm transactions ("mining")

- Users (●) are anonymous

- Each user has a copy of the legder and partipates in confirming transactions independently

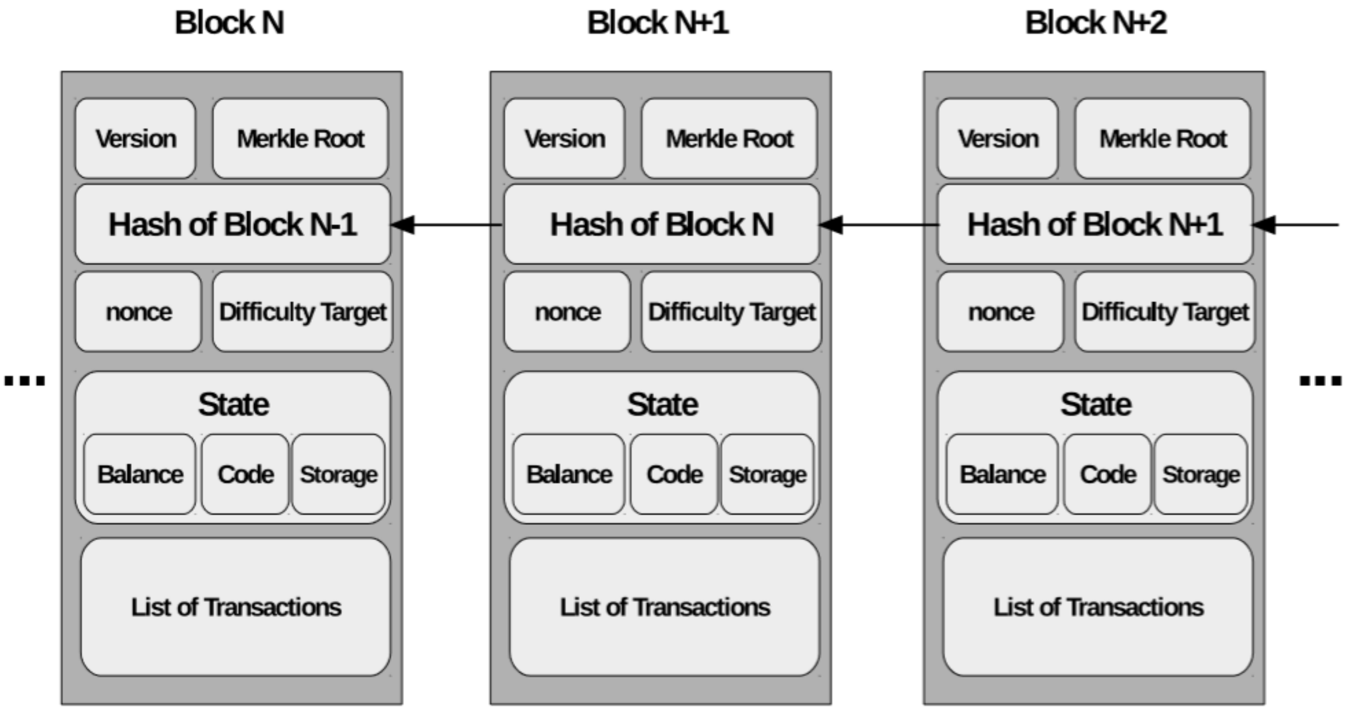
- Users (●) are not anonymous

- Permision is required for users to have a copy of the legder and participate in confirming transactions

Ref: https://blockgeeks.com/guides/what-is-blockchain-technology/

Background for understanding a blockchain

- Version : protocol version
- Merkle Root : hash value about List of Transactions
- **Hash of Block N-1 : hash value about previous block**
- nonce, Difficulty Target : additional data for consensus
- State : data for smart contract



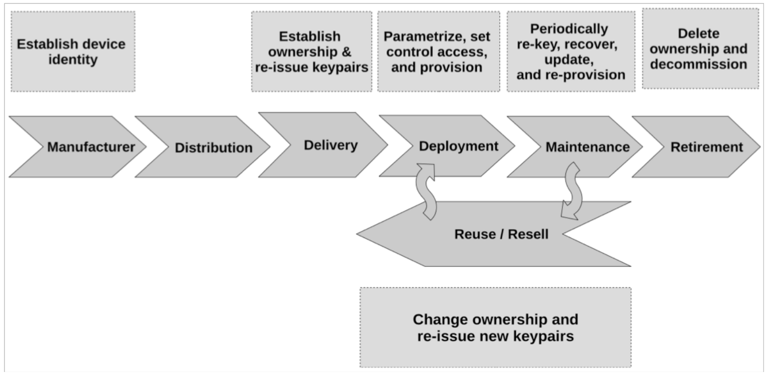
Potential blockchain solutions

- **Address Space**
  - Blockchain has a 160bit address space.
  - With 160-bit address, blockchain can generate and allocate address offline for around $1.46 * 10^{48}$ IoT devices.
  - The Probability of address collision is approximately 10^{48} , which is considered sufficiently secure to provide a Global Unique Identifier which requires no registration or uniqueness verification when assigning and allocating an address to an IoT device.

- **Identity of Things and Governance**
  - Blockchain has been used widely for providing trustworthy and authorized identity registration, ownership tracking and monitoring of products, goods, and assets.
  - Blockchain can be used to attributes and complex relationships that can be used to register and give identity to connected IoT device, with a set of attributes and complex relationships that can be uploaded and stored on the blockchain distributed ledger.

Potential blockchain solutions(Con't)

- **Data Authentication and Integrity**
  - data transmitted by IoT devices connected to the blockchain network will always be cryptographically proofed and signed by the true sender authentication and integrity of transmitted data.
- **Authentication, Authorization, and Privacy.**
  - smart contracts can provide a more effective authorization access rules to connected IoT devices with way less complexity when compared with traditional authorization protocols
  - The smart contracts can spell out also who has the right to update, upgrade, patch the IoT software or hardware, reset the IoT device, provision of new keypairs, initiate a service or repair request, change ownership, and provision or re-provision of the device.


Establish device identity
Establish ownership & re-issue keypairs
Parametrize, set control access, and provision
Periodically re-key, recover, update, and re-provision
Delete ownership and decommission
Manufacturer
Distribution
Delivery
Deployment
Maintenance
Retirement
Reuse / Resell
Change ownership and re-issue new keypairs

IoT device lifecycle security management

- **Secure Communications**
  - With blockchain, key management and distribution are totally eliminated, as each IoT device would have his own unique GUID and asymmetric key pair once installed and connected to the blockchain network.

Open challenges in IoT

- **Resource Limitations**
  - To be lightweight and energy efficient despite requiring complex computations along with improvement of energy harvesting techniques.

- **Heterogeneous devices**
  - A dynamically adaptable security framework requires intelligence, which is subject to the standardization of resources to be deployed in IoT architectures.

- **Interoperability of security protocols**
  - Within the global mechanism, an effective combination of security standards at each layer can then be defined through consideration of architectural constraints.

- **Single points of failure**
  - Research work would require mechanisms and standards to introduce redundancy while keeping in view the trade-off between the costs and reliability of the entire infrastructure.

Open challenges in IoT(Con't)

- **Hardware/firmware vulnerabilities**
  - Any vulnerabilities exploited after deployment become difficult to detect and alleviate. A standard verification protocol is therefore an essential requisite for harnessing the IoT security.

- **Trusted updates and management**
  - The issues related to secure and trusted governance of IoT device ownership, supply chain, and data privacy are open research problems that need to be addressed by the research community to foster a wide and massive scale adoption for IoT.

- **Blockchain vulnerabilities**
  - Effective mechanisms yet need to be defined to ensure the privacy of transactions and avoid race attacks which may result in double spending during transactions.

Summary

- IoT network is consist of resource-constrained devices, that is mainly why the IoT network is insecure and incapable of defending themselves.

- So, the authors conducted a survey about IoT security issues and categorized these issues depending upon IoT layers (Low-level layer, Intermediate-level layer, High-level layer).

- Also, they introduced some blockchain solutions for IoT security and explained how the blockchain can be used to solve IoT security issues.

- Despite there is a lot of efforts for IoT security, IoT still have the open challenges including resource limitations, heterogeneous devices, interoperability of security protocols, single points of failure, hardware/firmware vulnerabilities, trusted updates and management, blockchain vulnerabilities.

In my opinion…

- In this paper, there are no details about the schemes of blockchain solutions for IoT security.
- It was explained the directions of blockchain solutions and their advantages.
- However, the blockchain network has performance issues itself. And, in the IoT environment, there are too many devices. Therefore, It can result in a critical performance issue.
- Also, IoT with blockchains means that the IoT network inherits the existing blockchain security issues. As the IoT network is consist of resource-constrained devices, we may not adopt the existing solutions of blockchain security. it can be also another open problem.
- So, I think it would be a good direction to research the availability of blockchain in IoT network or analyze the possibility that the existing solutions for blockchain can be adopted to the IoT network.

THANK YOU FOR LISTENING

FINISH