Challanges of IoT

Internet of Things

Rahul Shandilya

Design Challanges

Heterogeneity and Interoperability

- Due to version upgrades and addition of new vendor products, the backend logic has to cater to a multi vendor or multi version deployment of IoT devices.

Design Challanges

Heterogeneity and Interoperability

- Due to version upgrades and addition of new vendor products, the backend logic has to cater to a multi vendor or multi version deployment of IoT devices.
- This can be achieved using an API translator. The API translation component can effectively expose a consistent set of APIs and message formats in one direction while using adapter sub-components to manage interoperability between heterogeneous devices.

Design Challanges

Heterogeneity and Interoperability

- Due to version upgrades and addition of new vendor products, the backend logic has to cater to a multi vendor or multi version deployment of IoT devices.
- This can be achieved using an API translator. The API translation component can effectively expose a consistent set of APIs and message formats in one direction while using adapter sub-components to manage interoperability between heterogeneous devices.
- The component thus has to be reachable from the field area devices and must therefore necessarily expose a public IP. By bombarding this component with bogus requests, it could be possible to induce the backend system into dedicated precious bandwidth towards executing bogus workloads, thus resulting in a service outage leading to DOS attacks.

Design Challanges

Heterogeneity and Interoperability

- Due to version upgrades and addition of new vendor products, the backend logic has to cater to a multi vendor or multi version deployment of IoT devices.
- This can be achieved using an API translator. The API translation component can effectively expose a consistent set of APIs and message formats in one direction while using adapter sub-components to manage interoperability between heterogeneous devices.
- The component thus has to be reachable from the field area devices and must therefore necessarily expose a public IP. By bombarding this component with bogus requests, it could be possible to induce the backend system into dedicated precious bandwidth towards executing bogus workloads, thus resulting in a service outage leading to DOS attacks.
- Spoofing is possible in this heterogeneous environment where a malicious node might impersonate another node possibly a router to route data through itself and get unauthorized access to sensor data.

Design Challanges

Heterogeneity and Interoperability

- Due to version upgrades and addition of new vendor products, the backend logic has to cater to a multi vendor or multi version deployment of IoT devices.
- This can be achieved using an API translator. The API translation component can effectively expose a consistent set of APIs and message formats in one direction while using adapter sub-components to manage interoperability between heterogeneous devices.
- The component thus has to be reachable from the field area devices and must therefore necessarily expose a public IP. By bombarding this component with bogus requests, it could be possible to induce the backend system into dedicated precious bandwidth towards executing bogus workloads, thus resulting in a service outage leading to DOS attacks.
- Spoofing is possible in this heterogeneous environment where a malicious node might impersonate another node possibly a router to route data through itself and get unauthorized access to sensor data.

Connectivity

- IoT applications typically require two forms of connectivity, and either of these have their own set of challenges.

Connectivity

- IoT applications typically require two forms of connectivity, and either of these have their own set of challenges.
- The first form is at a physical level, where the sender and receiver need to communicate using the same PHY and MAC

Connectivity

- IoT applications typically require two forms of connectivity, and either of these have their own set of challenges.
- The first form is at a physical level, where the sender and receiver need to communicate using the same PHY and MAC
- Unfortunately peripheral IOT devices tend to communicate over low power radio standards like Bluetooth, ZigBee, Z-Wave, NFC etc The information from these peripheral devices have to be bridged to an IP network over traditional Ethernet networks.The bridging devices act as proxies for the peripheral devices which may be a cause for MITM (man in the middle attack).

Connectivity

- IoT applications typically require two forms of connectivity, and either of these have their own set of challenges.
- The first form is at a physical level, where the sender and receiver need to communicate using the same PHY and MAC
- Unfortunately peripheral IOT devices tend to communicate over low power radio standards like Bluetooth, ZigBee, Z-Wave, NFC etc The information from these peripheral devices have to be bridged to an IP network over traditional Ethernet networks.The bridging devices act as proxies for the peripheral devices which may be a cause for MITM (man in the middle attack).
- The second form of connectivity is in terms of service connectivity. Even if packets from a physical device can reach the backend, it needs to be appropriately registered so that the backend can deliver these messages to the appropriate services.

Connectivity

- IoT applications typically require two forms of connectivity, and either of these have their own set of challenges.
- The first form is at a physical level, where the sender and receiver need to communicate using the same PHY and MAC
- Unfortunately peripheral IOT devices tend to communicate over low power radio standards like Bluetooth, ZigBee, Z-Wave, NFC etc The information from these peripheral devices have to be bridged to an IP network over traditional Ethernet networks.The bridging devices act as proxies for the peripheral devices which may be a cause for MITM (man in the middle attack).
- The second form of connectivity is in terms of service connectivity. Even if packets from a physical device can reach the backend, it needs to be appropriately registered so that the backend can deliver these messages to the appropriate services.
- Any kind of changes to the availability of the services has to be notified to the respective devices. Otherwise devices will unknowingly flood requests to an unavailable server leading to DOS attacks.

Mobility and Scalability

- As the mobility of devices in the field area increases, there could be frequent disruption in the physical connectivity between the devices with their local bridges.

Mobility and Scalability

- As the mobility of devices in the field area increases, there could be frequent disruption in the physical connectivity between the devices with their local bridges.
- To mitigate rogue devices from latching on to unauthorized services, peripheral devices that move to a new location have to maintain service continuity through secure handoff mechanisms.

Mobility and Scalability

- As the mobility of devices in the field area increases, there could be frequent disruption in the physical connectivity between the devices with their local bridges.
- To mitigate rogue devices from latching on to unauthorized services, peripheral devices that move to a new location have to maintain service continuity through secure handoff mechanisms.
- On the other hand, if the service continuity is disrupted, owing to the unavailability of the bridging infrastructure or other reasons, the isolated nodes must be extensively re-verified before the resumption of services.

Mobility and Scalability

- As the mobility of devices in the field area increases, there could be frequent disruption in the physical connectivity between the devices with their local bridges.
- To mitigate rogue devices from latching on to unauthorized services, peripheral devices that move to a new location have to maintain service continuity through secure handoff mechanisms.
- On the other hand, if the service continuity is disrupted, owing to the unavailability of the bridging infrastructure or other reasons, the isolated nodes must be extensively re-verified before the resumption of services.
- In most IoT applications it is sufficient to verify just the field devices, but in a few sensitive situations it might require two way verification of the backend system as well.

Mobility and Scalability

- As the mobility of devices in the field area increases, there could be frequent disruption in the physical connectivity between the devices with their local bridges.
- To mitigate rogue devices from latching on to unauthorized services, peripheral devices that move to a new location have to maintain service continuity through secure handoff mechanisms.
- On the other hand, if the service continuity is disrupted, owing to the unavailability of the bridging infrastructure or other reasons, the isolated nodes must be extensively re-verified before the resumption of services.
- In most IoT applications it is sufficient to verify just the field devices, but in a few sensitive situations it might require two way verification of the backend system as well.
- An adversary node might inject some malicious data in a roaming network before moving back to the home network and hide itself in the roaming network to promote repudiation attacks. Further a cloned node may illegally want to exploit the mobility to co-exist in another network

- Field deployments of IoT applications tend to grow either horizontally or vertically.

- Field deployments of IoT applications tend to grow either horizontally or vertically.
- In the case of horizontal scalability,hardware load balancers can be used extensively to improve service availability to the bridging infrastructure.

- Field deployments of IoT applications tend to grow either horizontally or vertically.
- In the case of horizontal scalability,hardware load balancers can be used extensively to improve service availability to the bridging infrastructure.
- It is thus important to allow only authorized devices to pass through.Otherwise, there is a potential for rouge nodes to launch DOS attacks by overwhelming the load balances.

- Field deployments of IoT applications tend to grow either horizontally or vertically.
- In the case of horizontal scalability,hardware load balancers can be used extensively to improve service availability to the bridging infrastructure.
- It is thus important to allow only authorized devices to pass through.Otherwise, there is a potential for rouge nodes to launch DOS attacks by overwhelming the load balances.
- Alternatively in the case of vertical scalability, the network can extend multiple hops. It is thus important to be able to trust intermediate nodes in the field area network. Otherwise, it has the potential to introduce sinkhole or wormhole attacks.

Addressing and Identification

- Field devices in IoT applications prefer to use low power radios for the last mile connectivity. As per current practices, coordinator nodes allocate local addresses to peer devices and these addresses do not follow a common standard.

Addressing and Identification

- Field devices in IoT applications prefer to use low power radios for the last mile connectivity. As per current practices, coordinator nodes allocate local addresses to peer devices and these addresses do not follow a common standard.
- Moreover the addressing scheme of a field network remains hidden behind the gateway/bridge, and makes it difficult to isolate a rogue node.

Addressing and Identification

- Field devices in IoT applications prefer to use low power radios for the last mile connectivity. As per current practices, coordinator nodes allocate local addresses to peer devices and these addresses do not follow a common standard.
- Moreover the addressing scheme of a field network remains hidden behind the gateway/bridge, and makes it difficult to isolate a rogue node.
- Since the node becomes untraceable, at a later point of time it might deny for sending a message and thus lead to repudiation attacks. Further the node can attempt to access unauthorised privileges remaining screened from the outside network.

Addressing and Identification

- Field devices in IoT applications prefer to use low power radios for the last mile connectivity. As per current practices, coordinator nodes allocate local addresses to peer devices and these addresses do not follow a common standard.
- Moreover the addressing scheme of a field network remains hidden behind the gateway/bridge, and makes it difficult to isolate a rogue node.
- Since the node becomes untraceable, at a later point of time it might deny for sending a message and thus lead to repudiation attacks. Further the node can attempt to access unauthorised privileges remaining screened from the outside network.
- Even it might take the advantage of not being traceable from the outside network and spoof within its network to other nodes claiming itself to be a genuine bridge of the network.

Addressing and Identification

- Field devices in IoT applications prefer to use low power radios for the last mile connectivity. As per current practices, coordinator nodes allocate local addresses to peer devices and these addresses do not follow a common standard.
- Moreover the addressing scheme of a field network remains hidden behind the gateway/bridge, and makes it difficult to isolate a rogue node.
- Since the node becomes untraceable, at a later point of time it might deny for sending a message and thus lead to repudiation attacks. Further the node can attempt to access unauthorised privileges remaining screened from the outside network.
- Even it might take the advantage of not being traceable from the outside network and spoof within its network to other nodes claiming itself to be a genuine bridge of the network.
- To address this problem, low power radios must support a common addressing scheme like 6LoWPAN that would enable each node to obtain a unique IPv6 address.

Addressing and Identification

- Field devices in IoT applications prefer to use low power radios for the last mile connectivity. As per current practices, coordinator nodes allocate local addresses to peer devices and these addresses do not follow a common standard.
- Moreover the addressing scheme of a field network remains hidden behind the gateway/bridge, and makes it difficult to isolate a rogue node.
- Since the node becomes untraceable, at a later point of time it might deny for sending a message and thus lead to repudiation attacks. Further the node can attempt to access unauthorised privileges remaining screened from the outside network.
- Even it might take the advantage of not being traceable from the outside network and spoof within its network to other nodes claiming itself to be a genuine bridge of the network.
- To address this problem, low power radios must support a common addressing scheme like 6LoWPAN that would enable each node to obtain a unique IPv6 address.
- For further security, there should be a global repository where device-IP mappings can be queried for authenticity by interested services or certificate providers.

Spatio-temporal services

- Any event in the IoT world can be characterized by the amplitude of a spatio-temporal impulse. Therefore it is necessary that the nodes in an IoT deployment are reasonably time synchronized and that they are able to tag any data with a spatial geolocation.

Spatio-temporal services

- Any event in the IoT world can be characterized by the amplitude of a spatio-temporal impulse. Therefore it is necessary that the nodes in an IoT deployment are reasonably time synchronized and that they are able to tag any data with a spatial geolocation.
- To achieve this end, these devices could leverage location services like GPS or Cell Tower Triangulation or WiFi triangulation.

Spatio-temporal services

- Any event in the IoT world can be characterized by the amplitude of a spatio-temporal impulse. Therefore it is necessary that the nodes in an IoT deployment are reasonably time synchronized and that they are able to tag any data with a spatial geolocation.
- To achieve this end, these devices could leverage location services like GPS or Cell Tower Triangulation or WiFi triangulation.
- But due to this feature, the user location data should not be revealed to unauthorised users as this might lead to privacy issues.

Spatio-temporal services

- Any event in the IoT world can be characterized by the amplitude of a spatio-temporal impulse. Therefore it is necessary that the nodes in an IoT deployment are reasonably time synchronized and that they are able to tag any data with a spatial geolocation.
- To achieve this end, these devices could leverage location services like GPS or Cell Tower Triangulation or WiFi triangulation.
- But due to this feature, the user location data should not be revealed to unauthorised users as this might lead to privacy issues.
- Also to ensure the time drifts within the FAN cannot be exploited for replay attacks, the APIs exposed by the backend system should ideally be idempotent.

Spatio-temporal services

- Any event in the IoT world can be characterized by the amplitude of a spatio-temporal impulse. Therefore it is necessary that the nodes in an IoT deployment are reasonably time synchronized and that they are able to tag any data with a spatial geolocation.
- To achieve this end, these devices could leverage location services like GPS or Cell Tower Triangulation or WiFi triangulation.
- But due to this feature, the user location data should not be revealed to unauthorised users as this might lead to privacy issues.
- Also to ensure the time drifts within the FAN cannot be exploited for replay attacks, the APIs exposed by the backend system should ideally be idempotent.
- Additionally the backend system must take into account the variance in the location data that is available from the end nodes. Otherwise it results in an inaccuracy of fault reporting leading to incorrect decisions.

Resource constraints

- A vast majority of peripheral IoT devices are resource constrained. The constraints could be in terms of available computational resources, onboard memory(RAM and ROM), network bandwidth, energy availability, etc.

Resource constraints

- A vast majority of peripheral IoT devices are resource constrained. The constraints could be in terms of available computational resources, onboard memory(RAM and ROM), network bandwidth, energy availability, etc.
- As these nodes are open in the environment and easily accessible physically, they can be cloned and tampered.

Resource constraints

- A vast majority of peripheral IoT devices are resource constrained. The constraints could be in terms of available computational resources, onboard memory(RAM and ROM), network bandwidth, energy availability, etc.
- As these nodes are open in the environment and easily accessible physically, they can be cloned and tampered.
- Also as these nodes have very little computation and storage capabilities, they preferably upload the data into the cloud for huge computations and storage. For this reason the user data privacy issues also creep in. So strong cryptographic encryption and integrity mechanisms need to be applied.

Data Interchange

- Each of the different devices in an IoT application can potentially have a different data packing mechanism because of specific optimizations on their hardware platform.

Data Interchange

- Each of the different devices in an IoT application can potentially have a different data packing mechanism because of specific optimizations on their hardware platform.
- If an encrypted packet is decrypted and repacked at multiple points in the communication chain, it opens up a security vulnerability including information leakage and user privacy because the keys are being shared between multiple devices.

Data Interchange

- Each of the different devices in an IoT application can potentially have a different data packing mechanism because of specific optimizations on their hardware platform.
- If an encrypted packet is decrypted and repacked at multiple points in the communication chain, it opens up a security vulnerability including information leakage and user privacy because the keys are being shared between multiple devices.
- Moreover, as the intermediary nodes are involved in crypto works they in turn become prone towards resource exhaustion and DOS attacks. For this reason end to end encryptions are better preferred.

Resource and service discovery

- In an IoT application it is expected that a large number of end devices are going to be deployed in the field. Therefore it is imperative that IoT devices can function autonomously and that they can discover the necessary services that they need to consume.

Resource and service discovery

- In an IoT application it is expected that a large number of end devices are going to be deployed in the field. Therefore it is imperative that IoT devices can function autonomously and that they can discover the necessary services that they need to consume.
- Therefore the coordinators in an IoT deployment must implement resource and service directories that can be queried on a public interface.

Resource and service discovery

- In an IoT application it is expected that a large number of end devices are going to be deployed in the field. Therefore it is imperative that IoT devices can function autonomously and that they can discover the necessary services that they need to consume.
- Therefore the coordinators in an IoT deployment must implement resource and service directories that can be queried on a public interface.
- The mechanisms like , two way authentication of the coordinators must be done to ensure that a rogue coordinator does not implement fake services and subsequently redirect traffic through itself and may lead to spoofing.

Resource and service discovery

- In an IoT application it is expected that a large number of end devices are going to be deployed in the field. Therefore it is imperative that IoT devices can function autonomously and that they can discover the necessary services that they need to consume.
- Therefore the coordinators in an IoT deployment must implement resource and service directories that can be queried on a public interface.
- The mechanisms like , two way authentication of the coordinators must be done to ensure that a rogue coordinator does not implement fake services and subsequently redirect traffic through itself and may lead to spoofing.
- Also due to this discovery mechanism, unnecessary requests to pretend to discover a resource causes DOS like attacks.

Resource and service discovery

- In an IoT application it is expected that a large number of end devices are going to be deployed in the field. Therefore it is imperative that IoT devices can function autonomously and that they can discover the necessary services that they need to consume.
- Therefore the coordinators in an IoT deployment must implement resource and service directories that can be queried on a public interface.
- The mechanisms like , two way authentication of the coordinators must be done to ensure that a rogue coordinator does not implement fake services and subsequently redirect traffic through itself and may lead to spoofing.
- Also due to this discovery mechanism, unnecessary requests to pretend to discover a resource causes DOS like attacks.
- As the IoT architecture is hugely distributed, the user data becomes distributed in the clouds. So without proper security measures it may lead to information leakage and user privacy issues. Accounting information inconsistencies may also arise here unless correct measures have been taken.

Security Challenges in IOT

Device or node end point physical security

- As the IoT nodes are very easily accessible in the open environment, they have the possibility to be tampered or cloned. To prevent this, tamper resistant hardware should be provided for these nodes.

Security Challenges in IOT

Device or node end point physical security

- As the IoT nodes are very easily accessible in the open environment, they have the possibility to be tampered or cloned. To prevent this, tamper resistant hardware should be provided for these nodes.
- Even if a node is tampered or compromised, there should be enough resiliency so that other nodes remain unaffected. Upon detection of a node being tampered, future communications with the node might be blocked to prevent further information loss.

Security Challenges in IOT

Device or node end point physical security

- As the IoT nodes are very easily accessible in the open environment, they have the possibility to be tampered or cloned. To prevent this, tamper resistant hardware should be provided for these nodes.
- Even if a node is tampered or compromised, there should be enough resiliency so that other nodes remain unaffected. Upon detection of a node being tampered, future communications with the node might be blocked to prevent further information loss.
- In the extreme case, the node may be needed to flush all data remotely so that the critical data are by no means accessed by illegal malicious nodes. Cloning of nodes can be prevented by allowing no access to its memory or crypto information from external sources.

Security Challenges in IOT

Bootstrapping and setup security

- While in the process of latching on to a network in the bootstrapping phase, the cipher and other critical information in the nodes should be kept secret.

Authentication, Access control and Accounting

Security Challenges in IOT

Bootstrapping and setup security

- While in the process of latching on to a network in the bootstrapping phase, the cipher and other critical information in the nodes should be kept secret.
- Typical cryptographic information including pre-shared keys and other private keys must not be compromised or stolen.

Authentication, Access control and Accounting

Security Challenges in IOT

Bootstrapping and setup security

- While in the process of latching on to a network in the bootstrapping phase, the cipher and other critical information in the nodes should be kept secret.
- Typical cryptographic information including pre-shared keys and other private keys must not be compromised or stolen.
- After the bootstrapping phase is done safely, the device may participate in establishing shared keys.

Authentication, Access control and Accounting

Security Challenges in IOT

Bootstrapping and setup security

- While in the process of latching on to a network in the bootstrapping phase, the cipher and other critical information in the nodes should be kept secret.
- Typical cryptographic information including pre-shared keys and other private keys must not be compromised or stolen.
- After the bootstrapping phase is done safely, the device may participate in establishing shared keys.

Authentication, Access control and Accounting

- Before any node communicates with a server, it should properly authenticate itself using certificates as well as the destination node to prevent open access to node data.

Security Challenges in IOT

Bootstrapping and setup security

- While in the process of latching on to a network in the bootstrapping phase, the cipher and other critical information in the nodes should be kept secret.
- Typical cryptographic information including pre-shared keys and other private keys must not be compromised or stolen.
- After the bootstrapping phase is done safely, the device may participate in establishing shared keys.

Authentication, Access control and Accounting

- Before any node communicates with a server, it should properly authenticate itself using certificates as well as the destination node to prevent open access to node data.
- Also justified authorization and access control rules are to be implemented on these nodes to limit them from super user access.

Security Challenges in IOT

Bootstrapping and setup security

- While in the process of latching on to a network in the bootstrapping phase, the cipher and other critical information in the nodes should be kept secret.
- Typical cryptographic information including pre-shared keys and other private keys must not be compromised or stolen.
- After the bootstrapping phase is done safely, the device may participate in establishing shared keys.

Authentication, Access control and Accounting

- Before any node communicates with a server, it should properly authenticate itself using certificates as well as the destination node to prevent open access to node data.
- Also justified authorization and access control rules are to be implemented on these nodes to limit them from super user access.
- At the end, detailed accounting information of the transaction should be logged. This way it will prevent to get exploited from spoofing, repudiation and privilege elevation attacks.

Data transmission and storage security

- Data while being transmitted over the network should be made secure by using the light-weight crypto algorithms tailored for these resource constrained networks.

Data transmission and storage security

- Data while being transmitted over the network should be made secure by using the light-weight crypto algorithms tailored for these resource constrained networks.
- Symmetric key encryptions are faster but PKI infrastructure though being slow allows dynamic key generation and distribution.

Data transmission and storage security

- Data while being transmitted over the network should be made secure by using the light-weight crypto algorithms tailored for these resource constrained networks.
- Symmetric key encryptions are faster but PKI infrastructure though being slow allows dynamic key generation and distribution.
- For integrity checks and to prevent against MITM attacks light-weight hashes and integrity check codes may be used.

Data transmission and storage security

- Data while being transmitted over the network should be made secure by using the light-weight crypto algorithms tailored for these resource constrained networks.
- Symmetric key encryptions are faster but PKI infrastructure though being slow allows dynamic key generation and distribution.
- For integrity checks and to prevent against MITM attacks light-weight hashes and integrity check codes may be used.
- Since the nodes have very less memory they can't store huge amounts of data or are capable of doing huge computations and thus off-load them to powerful cloud servers.

Data transmission and storage security

- Data while being transmitted over the network should be made secure by using the light-weight crypto algorithms tailored for these resource constrained networks.
- Symmetric key encryptions are faster but PKI infrastructure though being slow allows dynamic key generation and distribution.
- For integrity checks and to prevent against MITM attacks light-weight hashes and integrity check codes may be used.
- Since the nodes have very less memory they can't store huge amounts of data or are capable of doing huge computations and thus off-load them to powerful cloud servers.
- Stored data should be properly signed and encrypted so that they are genuine data and not readable by an anonymous entity.

Proxy security

- The proxies become a major target because data are transformed from one form to another.

Proxy security

- The proxies become a major target because data are transformed from one form to another.
- This bridging infrastructure is thus expected to provide decent transport level security by implementing something like a secure DTLS over 6LoWPAN on their FAN side and TLS on their ethernet side.

Proxy security

- The proxies become a major target because data are transformed from one form to another.
- This bridging infrastructure is thus expected to provide decent transport level security by implementing something like a secure DTLS over 6LoWPAN on their FAN side and TLS on their ethernet side.
- Secure interfaces and mechanisms of secure transit are required.

Proxy security

- The proxies become a major target because data are transformed from one form to another.
- This bridging infrastructure is thus expected to provide decent transport level security by implementing something like a secure DTLS over 6LoWPAN on their FAN side and TLS on their ethernet side.
- Secure interfaces and mechanisms of secure transit are required.
- Application level security can be built in addition to the transport layer security, depending on the capability of the hardware.

Proxy security

- The proxies become a major target because data are transformed from one form to another.
- This bridging infrastructure is thus expected to provide decent transport level security by implementing something like a secure DTLS over 6LoWPAN on their FAN side and TLS on their ethernet side.
- Secure interfaces and mechanisms of secure transit are required.
- Application level security can be built in addition to the transport layer security, depending on the capability of the hardware.
- Also cookie or nonce based mechanisms should be implemented to guard them against improper resource allocations and DOS attacks.

Proxy security

- The proxies become a major target because data are transformed from one form to another.
- This bridging infrastructure is thus expected to provide decent transport level security by implementing something like a secure DTLS over 6LoWPAN on their FAN side and TLS on their ethernet side.
- Secure interfaces and mechanisms of secure transit are required.
- Application level security can be built in addition to the transport layer security, depending on the capability of the hardware.
- Also cookie or nonce based mechanisms should be implemented to guard them against improper resource allocations and DOS attacks.
- Highly trust based systems are to work in these middle nodes and proxies.

Network and routing security

- The data while leaving a constrained network and being routed to the web from the router needs to be secure.

Network and routing security

- The data while leaving a constrained network and being routed to the web from the router needs to be secure.
- Data in transit in the network backbone should also be prevented from malicious activities. Corresponding encryption and integrity checks need to be implemented to guard against eaves dropping and data distortion attacks.

Network and routing security

- The data while leaving a constrained network and being routed to the web from the router needs to be secure.
- Data in transit in the network backbone should also be prevented from malicious activities. Corresponding encryption and integrity checks need to be implemented to guard against eaves dropping and data distortion attacks.
- Intrusion detection systems are essential to detect when a network has been adversely attacked and compromised by an attacker.

Network and routing security

- The data while leaving a constrained network and being routed to the web from the router needs to be secure.
- Data in transit in the network backbone should also be prevented from malicious activities. Corresponding encryption and integrity checks need to be implemented to guard against eaves dropping and data distortion attacks.
- Intrusion detection systems are essential to detect when a network has been adversely attacked and compromised by an attacker.
- Menwhile, corresponding prevention and rollback algorithms should be implemented to prevent the overall network from further damage.

Network and routing security

- The data while leaving a constrained network and being routed to the web from the router needs to be secure.
- Data in transit in the network backbone should also be prevented from malicious activities. Corresponding encryption and integrity checks need to be implemented to guard against eaves dropping and data distortion attacks.
- Intrusion detection systems are essential to detect when a network has been adversely attacked and compromised by an attacker.
- Menwhile, corresponding prevention and rollback algorithms should be implemented to prevent the overall network from further damage.
- Also the affected nodes should be isolated and investigated for the security breach.

Multi layer security

Higher layer protocols like (D)TLS, IpSec, etc. provide E2E security. But low powered devices latching with the gateway might run on 6LoWPAN and they in their network might need to adapt 802.15.4 link layer security. So the protocol stack should be flexible and accustomed with multiple security solutions while still maintaining the normal security requirements.

Common security measures

- To avoid DOS attacks stateless protocols would be a suitable alternative.

Multi layer security

Higher layer protocols like (D)TLS, IpSec, etc. provide E2E security. But low powered devices latching with the gateway might run on 6LoWPAN and they in their network might need to adapt 802.15.4 link layer security. So the protocol stack should be flexible and accustomed with multiple security solutions while still maintaining the normal security requirements.

Common security measures

- To avoid DOS attacks stateless protocols would be a suitable alternative.
- The loss due to spoofing can be limited by reducing the trust relationships, deep packet inspection and use anti-spoofing techniques.

Multi layer security

Higher layer protocols like (D)TLS, IpSec, etc. provide E2E security. But low powered devices latching with the gateway might run on 6LoWPAN and they in their network might need to adapt 802.15.4 link layer security. So the protocol stack should be flexible and accustomed with multiple security solutions while still maintaining the normal security requirements.

Common security measures

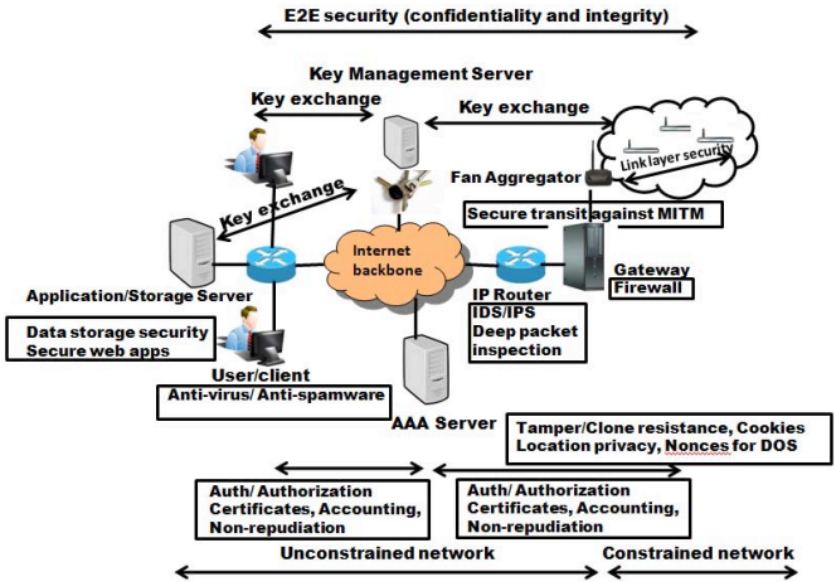
- To avoid DOS attacks stateless protocols would be a suitable alternative.
- The loss due to spoofing can be limited by reducing the trust relationships, deep packet inspection and use anti-spoofing techniques.
- Parties involved n MITM attacks should be guarded by using certificate authentications wherever possible and message integrity checks using MAC and MIC should be used.

- Software securities like firewall, IDS, context aware security measures and deep packet inspection techniques should be applied.

- Software securities like firewall, IDS, context aware security measures and deep packet inspection techniques should be applied.
- Anti-virus and antispamwares need to be deployed.

- Software securities like firewall, IDS, context aware security measures and deep packet inspection techniques should be applied.
- Anti-virus and antispamwares need to be deployed.
- Also application based web security protocols are valuable. Possible modifications are to be applied on the existing protocols to suite them in LLNs and also non-ip based systems.

- Software securities like firewall, IDS, context aware security measures and deep packet inspection techniques should be applied.
- Anti-virus and antispamwares need to be deployed.
- Also application based web security protocols are valuable. Possible modifications are to be applied on the existing protocols to suite them in LLNs and also non-ip based systems.
- Encryption, authentication, integrity, anti-replay, non-repudiation which stands as the basic mechanisms for security needs to be applied correspondingly but in a light-weight fashion to protect against the attacks.


E2E security (confidentiality and integrity)
Key Management Server
Key exchange
Key exchange
Key exchange
Link layer security
Fan Aggregator
Secure transit against MITM
Internet backbone
Gateway
Firewall
IP Router
IDS/IPS
Deep packet inspection
Application/Storage Server
Data storage security
Secure web apps
User/client
Anti-virus/ Anti-spamware
AAA Server
Tamper/Clone resistance, Cookies
Location privacy, Nonces for DOS
Auth/ Authorization
Certificates, Accounting,
Non-repudiation
Auth/ Authorization
Certificates, Accounting,
Non-repudiation
Unconstrained network
Constrained network

Other Challanges

Global cooperation

- The IoT can be claimed in the Chinese notion of “Sensing Planet” as “original” as any other vision available. It is able to integrate IoT fully into its technical architecture of the Future Internet.

Other Challanges

Global cooperation

- The IoT can be claimed in the Chinese notion of "Sensing Planet" as "original" as any other vision available. It is able to integrate IoT fully into its technical architecture of the Future Internet.
- A stakeholder approach in the EU that favors public-private partnerships and vertical investments through four-year program plans. The approach until now aimed to bring a broad adoption of potentially privacy-invading and business disruptive IoT as a set of applications.

Other Challanges

Global cooperation

- The IoT can be claimed in the Chinese notion of "Sensing Planet" as "original" as any other vision available. It is able to integrate IoT fully into its technical architecture of the Future Internet.
- A stakeholder approach in the EU that favors public-private partnerships and vertical investments through four-year program plans. The approach until now aimed to bring a broad adoption of potentially privacy-invading and business disruptive IoT as a set of applications.
- An opportunity investment approach in the US that is driven by short to mid-term return on investment. It is pushed by smart energy, smart cities, and RFID fueled by Department of Defense and Wal-Mart.

Business models, new currencies in IoT and trust

- IoT will lead to new “processes and innovative business models.”one model could be based on the idea of borrowing and lending objects instead of buying them.

Business models, new currencies in IoT and trust

- IoT will lead to new “processes and innovative business models.”one model could be based on the idea of borrowing and lending objects instead of buying them.
- A key area of research lies in building procedures and protocols for decision making that are not based on the premise of speed.

Business models, new currencies in IoT and trust

- IoT will lead to new "processes and innovative business models."one model could be based on the idea of borrowing and lending objects instead of buying them.
- A key area of research lies in building procedures and protocols for decision making that are not based on the premise of speed.
- In a real-time world there is no longer gain being the "first" to have the data. Instead, the internet of things favors a daily situation of full traceability.

Business models, new currencies in IoT and trust

- IoT will lead to new "processes and innovative business models."one model could be based on the idea of borrowing and lending objects instead of buying them.
- A key area of research lies in building procedures and protocols for decision making that are not based on the premise of speed.
- In a real-time world there is no longer gain being the "first" to have the data. Instead, the internet of things favors a daily situation of full traceability.
- There is so much contextual information about what you are wearing – this jacket or this pair of jeans – that neither the customer nor the merchant, require a Point of Sale/Point of Transaction as a "closure". And yet "closure" is of great importance to us as human beings, as it signals the "right" kind of feedback in a procedure enhancing levels of trust.

Business models, new currencies in IoT and trust

- IoT will lead to new "processes and innovative business models."one model could be based on the idea of borrowing and lending objects instead of buying them.
- A key area of research lies in building procedures and protocols for decision making that are not based on the premise of speed.
- In a real-time world there is no longer gain being the "first" to have the data. Instead, the internet of things favors a daily situation of full traceability.
- There is so much contextual information about what you are wearing – this jacket or this pair of jeans – that neither the customer nor the merchant, require a Point of Sale/Point of Transaction as a "closure". And yet "closure" is of great importance to us as human beings, as it signals the "right" kind of feedback in a procedure enhancing levels of trust.
- It may be the case that IoT will favor a situation where different forms of currencies, standards of banking and money will exist together

Ethics, control society, surveillance, consent and data driven life

- Privacy was named by the originator of ubicomp, Mark Weiser, the late chief scientist at Xerox Parc as a key issue.

Ethics, control society, surveillance, consent and data driven life

- Privacy was named by the originator of ubicomp, Mark Weiser, the late chief scientist at Xerox Parc as a key issue.
- Privacy is a key challenge that people may have about living in a future connected environment

Ethics, control society, surveillance, consent and data driven life

- Privacy was named by the originator of ubicomp, Mark Weiser, the late chief scientist at Xerox Parc as a key issue.
- Privacy is a key challenge that people may have about living in a future connected environment
- Privacy Enhancing Technologies (PET) is a partial solution. The Privacy Coach, produced by a small Dutch consortium of RFID experts, is an application running on a mobile phone that supports customers in making privacy decisions when confronted with RFID tags

Finding the perfect balance between top down planning and bottom up innovation

- IoT applications should be aimed to help the current institutions and public bodies to transform peacefully into a networked model of open data [6], direct feedback on where money goes, participatory budgeting models (say 25% for innovation in your street and neighborhood)

Finding the perfect balance between top down planning and bottom up innovation

- IoT applications should be aimed to help the current institutions and public bodies to transform peacefully into a networked model of open data [6], direct feedback on where money goes, participatory budgeting models (say 25% for innovation in your street and neighborhood)
- IoT could be extremely relevant in making direct feedback visible in street and city furniture, and mobile applications.

Finding the perfect balance between top down planning and bottom up innovation

- IoT applications should be aimed to help the current institutions and public bodies to transform peacefully into a networked model of open data [6], direct feedback on where money goes, participatory budgeting models (say 25% for innovation in your street and neighborhood)
- IoT could be extremely relevant in making direct feedback visible in street and city furniture, and mobile applications.
- The internet of things can be a layer of data, open to all, through which individuals can decide for themselves what they are willing to pay for, get direct feedback from their voluntary donations, coordinate community spending that has a direct bearing to their needs through participatory budgeting