Name : Azamuddin
Rotation Project Title : Survey on IoT Security

Outline :

- Abstract
- Introduction
- IoT
- Why Cyber Security Matters in Iot
- Types of Attacks and Threats
- Security Implementation on IoT
- ❑ WirelessHART Protocol
- ❑ Routing Attacks and Countermeasures in the RPL-Based Internet of Things (6LoWPAN)
- ❑ Link-Layer Security (IEEE 802.15.4)
- ❑ IoT Network Layer Security (IPSec)
- ❑ Embedded Security for Internet of Things
- Summary
- References

Abstract

The Internet of Things (IoT) is the development production of the computer science and communication technology. As IoT is broadly used in many fields, the security of IoT is becoming especially important and will take great effects on the industry of IoT….

Introduction

In recent years, with the development of computer science, communication technology and perception recognition technology, the network of things has made a great breakthrough. The IoT can find applications in many fields, from the earliest wireless sensor networks such as the smart grid, smart healthcare, smart agriculture, smart logistics and so on. …

Current Internet security protocols rely on a well-known and widely trusted suite of cryptographic algorithms: the Advanced Encryption Standard (AES) block cipher for confidentiality; the Rivest-Shamir-Adelman (RSA) asymmetric algorithm for digital signatures and key transport; the Diffie-Hellman (DH) asymmetric key agreement algorithm; and the SHA-1 and SHA-256 secure hash algorithms. This suite of algorithms is supplemented by a set of emerging asymmetric algorithms, known as Elliptic Curve Cryptography (ECC)….

- As reported by Anna Johansson at TechnologyTell, iControl, who provides the software plumbing for some of the largest home security vendors, recently published a study on the Smarthome. The results were conclusive regarding home security:
- 90% of respondents ranked home security as one of the most important elements of the Smarthome.
- 67% ranked home security as the most important element.

- *100% said that* ***they wouldn't install*** *a Smarthome* ***system if it didn't include home security.***

Findings : Security Implementation on IoT

The tables as shown below summarize and differentiate five IoT protocols in term of security goals, security threats security, technique used and design challenge.

WirelessHart	***6LoWPAN***	***IEEE 802.15.4***	***IPSEc***	***Embedded Security***
Protocol for industrial wireless sensor networks To avoid device cloning and stealing security secrets. Provides end-to-end and hop-to-hop security measures through payload encryption and message authentication on the Network and Data-link layers.	It designed to operate in a network environment with large number of embedded sensor devices over low data-rate and lossy wireless link. Such criteria are specified in the routing requirements defined in RFC 5867, 5826, 5673 and 5548.	Provides standardized mechanisms for message authentication and encryption on a per-hop base in 6LoWPAN networks.	IPsec in transport mode provides end-to-end security with authentication and replay protection services in addition to confidentiality and integrity. Psec ensures the confidentiality and integrity of the IP payload using the Encapsulated Security Payload (ESP) protocol, and integrity of the IP header plus payload using the Authentication Header (AH) protocol.	protecting the secrecy
It uses CCM* [2] mode in conjunction with AES- 128 block cipher using symmetric keys, for the message authentication	IP Connectivity mainly aim at protecting the communications from the end-users to the sensor network.			Secure Boot is to bring the system to a known and trusted state

and encryption. WirelessHART gateway and the wireless sensors joining the network must be configured to control which devices are allowed to access the network.				
WirelessHART gateway therefore has a secure authentication process which it uses to negotiate with all joining devices to ensure they are legitimate. As with all other network communications, all join negotiation traffic is encrypted end-to-end.	6LoWPAN routing protocol must satisfy the following: (i) support different types of communication Unicast/anycast/multicast; (ii) adaptive routing with different network condition; (iii) constraint-based; (iv) support different traffic: multipoint-to-point (sensor nodes to sink manner), point-to-multipoint (sink broadcasts) and point-to-point traffic (sensor nodes communicate to each other); (v) scalability; (vi) configuration and management; (vii) node attribute; (viii) performance; and (iv) security. Rank attack (RPL) Local repair attack Resource depleting attack			Secure content User identification

Table 1 : Security Goals

Features	***WirelessHart***	***6LoWPAN***	***IEEE 802.15.4***	***IPSEc***	***Embedded Security***
Confidentiality	Spoofing Eavesdroping Cloning		Tempering Eavesdroping Replay attack	Spoofing Eavesdroping	Temper proofing
Integrity	DoS Jamming Sybil Attack De-Synchronization Wormhole Tampering Exhaustion Selective Forwarding Collision	The attacks can be classified by several schemes: outsider–insider adverse source, passive–active, compromising methods, host-based or network-based.		DDoS attack	Cryptanalysis Attack Software Attacks
Availability	Denial of Service Failed access attempts Message integrity check failures Authentication failures	Routing attack Flooding Sinkhole attack Selective forwarding Local repair attack Resource depleting attack	Security threats from wireless sensor network side Security threats from the internet side Security threats from the routing protocol for low-power	Botnets	Malware and side channel attack Physical Attack Side Channal Attacks

			and lossy network		

Table 2 : Security Threats

WirelessHart	***6LoWPAN***	***IEEE 802.15.4***	***IPSEc***	***Embedded Security***
bidirectional network of relatively powerful devices and has a central network manager and controller As of version 7, HART also incorporates an IEEE 802.15.4-based wireless mesh network as an option for the physical layer.	Per-hop security with at least integrity protection should be used in 6LoWPAN networks to prevent unauthorized access through the radio medium, and to defend against effortless attacks launched to waste constrained resources.	for message authentication and encryption on a per-hop base in 6LoWPAN networks.	The most known algorithms are MD5 and SHA. In addition, non-repudiation, availability and authenticity are guaranteed by communication protocols like IPSec for example.	The hash of information is used to check the integrity of a message by providing a signature which is unique for each message. The most known algorithms are MD5 and SHA.
WirelessHART Security Manager	Cryptography techniques Intrusion detection system techniques	protects a communication on a per-hop base where every node in the communication path has to be trusted. A single pre-shared key is used to protect all communication.		multiple independent processor cores, secondary bus masters such as DMA engines, and large numbers of memory and peripheral bus slaves.

		In case an attacker compromises one device it gains access to the key, and the security of the whole network is compromised.		
	IDS protection layers	Roman et al. proposed key management systems for sensor network in the context of the IoT that are applicable to link-layer security.		In order to provide security at the physical or execution level, it need to build our solution based on secure execution environment (SEE). An SEE is a processing unit which is capable of executing applications in a protected manner, meaning the attacks originating from outside the SEE cannot tamper with code and data belonging to the SEE. The first building block of an SEE is of course a secure processor – either a dedicated processor or one capable of supporting a secure mode, which is hardware compartmentalized from the non-secure mode. Utilizing a dedicated

				processor has the advantage of ease of separation as well as offloading the main processor from handling security tasks. The disadvantage of a dedicated processor is the increase in silicon footprint
				Cryptographic Algorithms

Table 3 : Security Technique Used

WirelessHart	6LoWPAN	IEEE 802.15.4	IPSEc	Embedded Security
It does not support public key cryptography which makes it unable to provide certain security services such as non-repudiation. Strong authentication, i.e. authentication without sending the security secrets over the network is not possible either.	Per-hop security can detect the message modification on each hop unlike E2E where modified packets traverse the entire path up to the destination to be detected.	Difficult to implement on resource constrained sensor nodes.	most IPsec solutions for setting up Virtual Private Networks (VPN) require third-party hardware and/or software. Moreover, in order to access an IPsec VPN, a given endpoint must have an IPsec client application installed. This is both an asset and a drawback.	embedded security needs good amount of attention is: in-vehicular security. Security can be resource consuming and if we are using low power embedded device, this can be a big challenge. The computation power available in IoT is limited and may be insufficient for the processing of security algorithms. The battery capacity is also limited and their life duration is strongly connected to the quantity of computation executed in the embedded processor. Storage limitations also are hurdles for embedding security features.
No mechanisms have been	This system requires a lot of computational	cryptographic mechanisms can be		As heterogeneity increases, developing applications that run

specified to provide authorization and accounting security services. need accounting when the cost of WirelessHART device is attached to its usage.	loads with the three checking modules and another matching part so it will reduce the detection speed. The author did not explain why they chose to analyse only the data, which is discarded from the buffer. By doing that they probably assumed the data that passed to the buffer are attack-free while there is no guarantee in reality.	expensive in terms of code size and processing speed.		across all platforms will become exceedingly difficult which raises the need for standard interoperable security protocols.
The complete key management system is not specified; however, the commands for distribution of keys have been specified.				Cryptography is notoriously expensive and it makes security impossible for resource constrained devices. There is a need for optimized lightweight cryptographic algorithms for such devices.
Security in the wired part of the network is neither specified nor enforced. Secure multicast communication among the Field devices is not supported.	RPL specification-based IDS for securing network topology			The complexity and size of some protocols and algorithms makes security expensive.

The architecture of the Security Manager and the interface between the Security Manager and the Network Manager is not specified in the standard.				No “correct” solution. Security is based upon applications itself and it really varies radically from application to application.

Table 4 : Design Challenge

Service	Compressed IPsec		802.15.4 link layer security	
	Mode	Overhead	Mode	Overhead
Integrity	HMAC-SHAI-96	16B	AES-CBC-MAC-96	12 B X n frags
Confidentality	AES-CBC	12B	AES-CTR	5 B X n frags
Integrity and Confidentiality	AES-CBC AND HMAC-SHAI-96	26B	AES-CCM-128	21 B x n frags

IPSec vs. IEEE 802.15.4

An IPsec-based Security

IPsec (Internet Protocol Security) is a framework for a set of protocols for security at the network or packet processing layer of network communication.

Earlier security approaches have inserted security at the Application layer of the communications model. IPsec is said to be especially useful for implementing virtual private networks and for remote user access through dial-up connection to private networks. A big advantage of IPsec is that security arrangements can be handled without requiring changes to individual user computers. Cisco has been a leader in proposing IPsec as a standard (or combination of standards and technologies) and has included support for it in its network routers.
IPsec provides two choices of security service: Authentication Header (AH), which essentially allows authentication of the sender of data, and Encapsulating Security Payload (ESP), which supports both authentication of the sender and encryption of data as well. The specific information associated with each of these services is inserted into the packet in a header that

follows the IP packet header. Separate key protocols can be selected, such as the ISAKMP/Oakley protocol.

IP-based security solutions

In the context of the IP-based IoT solutions, consideration of TCP/IP security protocols is important as these protocols are designed to the IP network ideology and technology. While a wide range of specialized as well as general-purpose key exchange and security solutions exist for the Internet domain, I focus on the discussion of IKEv2/IPsec.

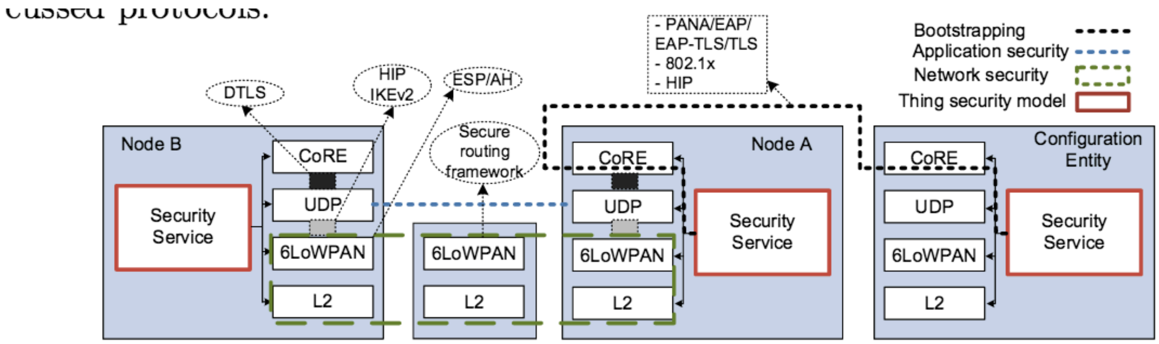


Fig. 3. Relationships between IP-based security protocols

The Internet Key Exchange (IKEv2)/IPsec and the Host Identity Protocol(HIP) reside at or above the network layer in the OSI model. Both protocols are able to perform an authenticated key exchange and set up the IPsec transform for secure payload delivery.

The Extensible Authentication Protocol (EAP) is an authentication frame-work supporting multiple authentication methods (?). EAP runs directly over the data link layer and, thus, does not require the deployment of IP. It supports duplicate detection and retransmission, but does not allow for packet fragmentation. The Protocol for Carrying Authentication for Network Access (PANA)

is a network-layer transport for EAP that enables network access authentication between clients and the network infrastructure. In EAP terms, PANA is a UDP-based EAP lower layer that runs between the EAP peer and the EAP authenticator.

In the Internet and hence in the IoT, security at the network layer is provided by the IP Security (IPsec) protocol suite. IPsec in transport mode provides end-to-end security with authentication and replay protection services in addition to confidentiality and integrity. By operating at the network layer, IPsec can be used with any transport layer protocol including TCP, UDP, HTTP, and CoAP. IPsec ensures the confidentiality and integrity of the IP payload using the Encapsulated Security Payload (ESP) protocol, and integrity of the IP header plus payload using the Authentication Header (AH) protocol. IPsec is mandatory in the IPv6 protocol meaning that all IPv6 ready devices by default have IPsec support, which may be enabled at any time. Being a network layer solution, IPsec security services are shared among all applications running on a particular machine. However, being mandatory in IPv6, IPsec is one of the most suitable options for E2E security in the IoT.

Work form (?) discuss an example for the establishment of an end-to-end secure communication channel between a Constrained Device (CD) and an Unconstrained Device (UD) with the following assumptions:

- The constrained node uses 6LoWPAN for addressing and CoAP as the application layer protocol.
- The unconstrained node uses IPv6 for addressing and HTTP as the application layer protocol.
- The constrained node is already authenticated with the Gateway (GW).
- There exists a security policy allowing secure communications within the constrained network domain (and in particular between GW and CD).
- The gateway is a trusted entity.

It is possible for an unconstrained node to set up an IPsec-ESP Transport Mode connection with an IoT device while moving the master session key generation and authentication processes from the IoT node to the trusted gateway. The ESP mode, which provides data encryption and authentication, allows the setup of an end-to-end secure connection between two peers by encrypting the payload, while leaving the IPv6 headers untouched. The cryptographic keys are generated and exchanged according to the IKE protocol using the Elliptic Curve Diffie Hellman key exchange scheme. With the aid of these mechanisms, the logic for key generation and authentication is moved from the IoT node to the corresponding GW, thus relieving the IoT device from the computational burden associated with the generation of cryptographic data. Fig. 6 illustrates the relevant steps involved in the procedure.

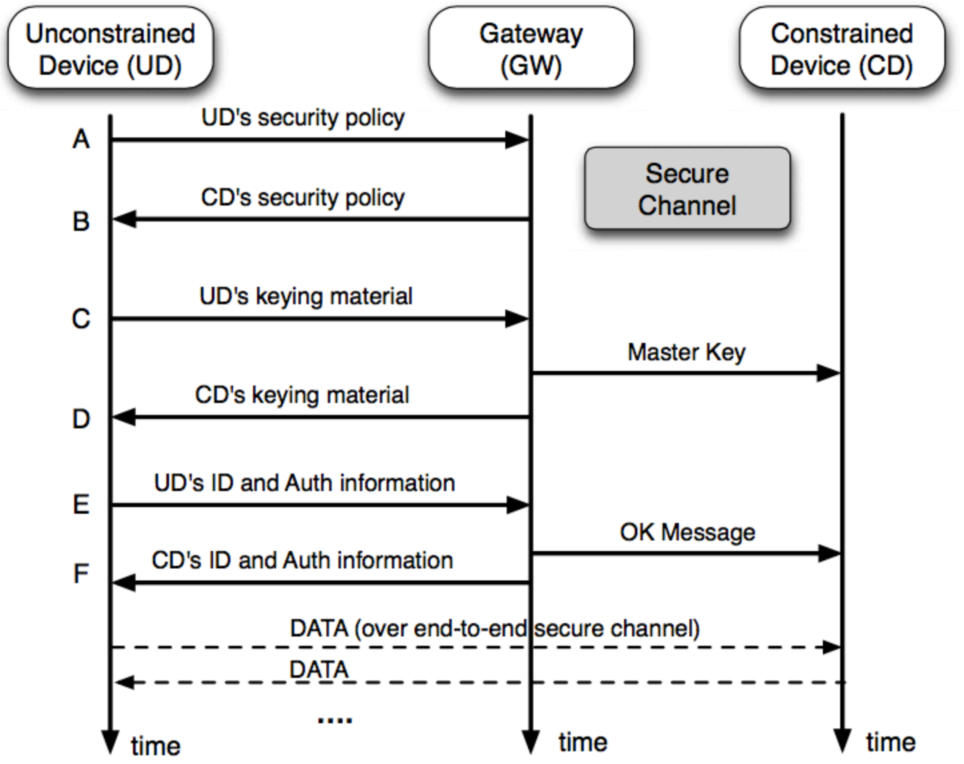


Figure 6. Lightweight IPsec security association.

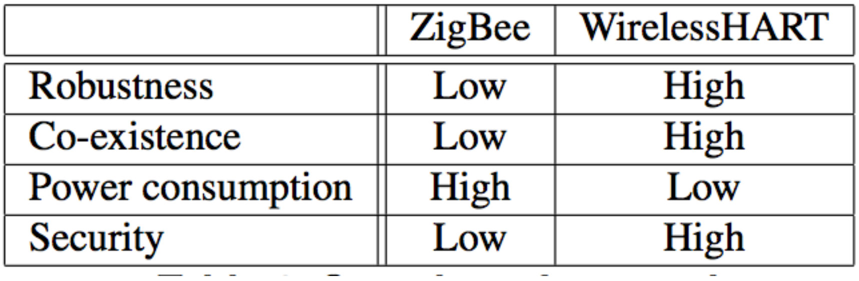
WirelessHART

WirelessHART is a secure protocol and provides several layers of protection (?). All traffic is secured, the payload is encrypted and all messages are authenticated, both on a singlehop basis as well as end-to-end. WirelessHART requires that all devices are provisioned with a secret Join key as well as a Network id in order to join the network.

WirelessHART, though resource constrained, is a bidirectional network of relatively powerful devices and has a central network manager and controller. WirelessHART, currently the only WSN standard, designed primarily for industrial process automation and control, is well designed for other aspects than security. The provided security is spread throughout the WirelessHART specifications. The network designers and device vendors have ambiguities regarding the complete security architecture of the WirelessHART, the strength of the provided security, the security keys needed, and the functionalities and placement of Security Manager.

A set of different security keys are used to ensure secure communication. A new device is provisioned with a *Join key* before it attempts to join the wireless network. The Join key is used to authenticate the device for a specific WirelessHART network. Once the device has successfully joined the network, the Network manager will provide it with proper Session and Network keys for further communication. The actual key generation and management is handled by a "plant wide" Security manager, which is not specified by WirelessHART, but the keys are distributed to the Network devices by the Network manager. A *Session key* is used by the Network layer to authenticate the end-to-end communication between two devices (e.g., a Field device and the Gateway). Different Session keys are used for each pairwise communication (e.g., Field device to Gateway, Field device to Network manager, etc). The Data Link layer uses a Network key to authenticate messages on a one-hop basis. A well known Network key is used when a device attempts to join the network, i.e., it before it has received a proper Network key. Keys are rotated based on the security procedures of the process automation plant.

Three key types are used: Master key, Link key and Network key. The master key is comparable to the join key in WirelessHART and is necessary to join the network. The link key is used for end-to-end encryption and would by that provide the highest level of security at the price of higher storage requirements. The network key is shared between all devices, and thus presents a lower level of security, though with the benefit of reduced storage requirements in the devices. All keys can be set at the factory, or be handed out from the trust center (residing in the network coordinator), either over the air, or through a physical interface. For commercial grade application, the trust center can control the joining of new devices and periodically refresh the network key(?).



	ZigBee	WirelessHART
Robustness	Low	High
Co-existence	Low	High
Power consumption	High	Low
Security	Low	High

Thomas et, al. (?) stated that *WirelessHART more suitable for industrial applications and requirements compare to ZigBee.*

6LowPAN

6LoWPAN security requirements

The RFC4919, specifies a list of security requirements for 6LoWPAN, which mainly aim at protecting the communications from the end-users to the sensor network. The requirement list is:

- Confidentiality: only authorised users can access the information
- Authentication: data is only originated from a trusted sources
- Integrity: the received data remains unchanged during transmission
- Freshness: consider for both data and key to ensure no replayed of old messages
- Availability : guarantee the data can be accessible when needed
- Robustness: providing operation despite the abnormal conditions
- Resiliency: provide an acceptable level of security even in the case some nodes are compromised
- Energy efficiency: reduce the control overhead to maximise network lifetime
- Assurance: the ability to disseminate different information. These requirements require the combination of different securing systems. Cryptography is considered the first line for solving the confidentiality, authentication and integrity. This system, how- ever, cannot solve other QoS securing requirements like availability, robustness and resiliency. It therefore needs to cooperate with the IDS, which can monitor and detect malicious sources from the early phase to eliminate further damage of the attacks.

Cryptography techniques

By encrypting messages before transmitting, the cryptography solutions aim at threefold protection: authentication only the authenticated user, who has the right key, can decrypt and read the messages; integrity message content should not be changed during transmission; and confidentiality. no one can understand the message without the key.

The encryption methods for 6LoWPAN should be developed more to adapt to the prevailing constraints in 6LoWPAN devices such as low power and low computing ability. This is because unoptimised cryptography mechanisms will consume more resources and therefore, shorten network life time. The key used in encryption methods should also not be too short; otherwise it will be easy to be broken by the attackers. Because 6LoWPAN is the combination of WSN and the Internet, it is natural to apply these two network cryptography mechanisms for securing this network. WSN uses AES (Advanced Encryption Standard) for securing the link layer with several operation modes, most of which does not ensure integrity function (?). To protect network layer end-to-end security, IPsec (Internet Protocol Security) is utilised with transport and tunnel modes. Before, the public key cryptography mechanism was thought to be too heavy for applying in WSN. However, recent research developments showed ways to combine RSA (Rivest - Shamir - Adelman asymmetric encryption) and ECC (Elliptic Curve Cryptography) techniques with several modes to adjust to network scenarios.

Exchanging key is another problem that should be considered. The Internet Key Exchange from IPsec (Internet Protocol Security) is suggested for exchanging the key in the network. However, the Internet Key Exchange is not considered as a feasible solution because of its heavy signalling messages, which is unsuitable for the small packet size of 802.15.4 nature and the energy efficiency requirement. The WSN used several key distribution methods like predistribute and key pool, however, they lack scalable ability. It is also necessary to analyse the threat towards the key at the bootstrap time when an adversary sits among other nodes without being required to be authenticated.

Although research shows significant improvements in using cryptography for 6LoWPAN, the network still has to overcome many problems. Cryptography is also only helpful while protect- ing 6LoWPAN from the external attacks, but lack the ability in detecting and eliminating internal attacks. This is because cryptography cannot detect attackers with legal keys but behave maliciously. Network security, which utilise only cryptography, is therefore weak under attacks aimed at network performance such as DoS or battery, and resource attacks like jamming and exhaust attack.

Cryptography alone, therefore, cannot provide total security for 6LoWPAN. There is a need for implementing IDS to monitor any malicious behaviour of the network to prevent early security attacks to decrease its effects. IDS is an efficient way for discovering any attacker that bypasses the cryptography defence line, and ensuring a normal operation of the network.

The combination of cryptography as the first line and IDS as the second line defence can secure the network from most of the threats. The missions of the IDS are to monitor and raise an alarm about any possible threats and pass it to the cryptography to restart the keying process for elim- inating the attackers. IDS can deal with all the threats (?)

Intrusion detection system techniques

Overview of intrusion detection system.

The intrusion detection system is a well-known net- work security approach that has attracted research interest since the 1970s (?). The main idea behind IDS is to collect the network data and analyse any sign of the attack to raise an alarm and discover the adverse resource.

The development of technology has changed the communication environment from wired, wireless, ad hoc to sensor network recently. IDS solutions have also changed from data collection and analysis techniques to adaptation to the implemented environment. The nature of WSN is different from other networks in terms of device communication ability and resource available. IDS applied in WSN should optimise the features and computational work for saving network resource.

With regard to 6LoWPAN, the optimisation ability of the IDS is even more required because of the network scalability.

The IDS approaches are often divided by misuse, anomaly-based and specification-based type. A misuse IDS first defines patterns of the known attacks, and when monitoring the network, if it discovers any data that match the pattern, it will raise a security alarm. This method can provide low-false alarm rate, but it needs to store a lot of data to be analysed, requires the attacks to be well defined and limits in detecting the new attacks. This approach is not favoured in WSN or 6LoWPAN because the knowledge about attacks is not well studied, security resource is constrained, and the network requires the ability to detect novel attacks.

Application of intrusion detections system in 6LoWPAN.

Cryptography solutions focus on choosing a fast, light-weight and secured encryption, and an effective key management method. Even when 6LoWPAN has an ideal cryptography line defence, there is still a need for implementing an IDS for dealing with network performance threats such as DoS and other resource attacks (?). The IDS will discover and stop most of the attacks that break cryptography protection to make changes on the network operation. However, no IDS solution has been proposed for 6LoWPAN security. This part takes the natural characteristics of 6LoWPAN to analyse the difference to other networks to clarify a 6LoWPAN IDS.

Intrusion detection system issues in wireless sensor network part.

Intrusion detection system solutions in WSN have to be light weight and low work load because of the resources constraint of the nodes. Their main issues are (i) the feature extraction: the issue in choosing the right features for reducing the monitored data and effectively detect the attacks; (ii) the placement problems: where to put the IDS agent in the network for an optimised operation; and (iii) the data analysis techniques: choosing a technique to increase accuracy and decrease the computational work.

To detect WSN attacks, a number of data features were proposed. Da Silva *et al.* (?) suggested to monitor: (i) the time between two consecutive messages for detecting the negligence (sending mes- sage too slowly) or exhaustion (sending message too quickly); (ii) payload: for discovering integrity attacks, which makes changes on payload; (iii) delay: detect attacks that make high delay in sending the messages such as black hole or selective forwarding; (iv) repetition: detect DoS attack; (v) senderID: for detecting wormhole, Helloflood attack — this parameter can also be applied in discovering Neighbour Discovery attacks of IPv6 and Sybil, which create a strange SenderID; and (vi) number of collisions: detect attacks that cause large number of collisions such as jamming attacks. Strikos (?) added the following parameters: (i) number of lost packets: higher of packet lost

Intrusion detection system issues in IPv6 part.

The IDS from IPv6 side is to protect the border router from any threats that send packets from IPv6 to WSN to start a WSN attack. Most of the issues in WSN parts are easy to solve in the IPv6 part because the border router is usually implemented with strong security and nonresource constraint and moreover, the threats that come from the IPv6 network are much less than threats inside the sensor network. For instance, the border router is the most suitable position to put the IDS agent because it is the place where the traffic between the two networks goes. The feature extraction issue is also not restricted like in the WSN part because of the high capacity of the border router. The only issue that needs to be focused on is choosing suitable IDS techniques for detecting threats early and accurately.

Again three types of methods: misuse, anomaly and specification-based can be applied. The misuse direction is still not favourable because no attack signatures are defined. Amin *et al.* (?) mentioned an IDS that can be considered as the combination of anomaly and misuse techniques. It uses the three techniques: Anderson-Darling Algorithm, Entropy Algorithm and PAT (Predefined Attack Types) calculator for detecting the abnormal behaviours. The chosen data feature is the dis- card packets from the congestion avoidance algorithms when the queues are full. To reduce the false alarm rate, they bring the discovered anomaly data to a pattern classifier, which checks the predefined attack type on the stored buffer. A threshold is also chosen for generating a security alert once it is detected to be passed by the classifier. This system requires a lot of computational loads with the three checking modules and another matching part so it will reduce the detection speed. The author did not explain why they chose to analyse only the data, which is discarded from the buffer. By doing that they probably assumed the data that passed to the buffer are attack-free while there is no guarantee in reality. The main architecture of this system, however, can still be applied with different detecting techniques for a better solution.

Security threats from wireless sensor network side

The security threats of WSN have been extensively studied by the research community. The attacks can be classified by several schemes: outsider–insider adverse source, passive–active, compromising methods, host-based or network-based (?).

From the protecting threat's point of view, detecting the attacks from the outsider and insider requires different protecting systems. The attackers outside of the network can initiate a passive attack such as unauthorised listening or active attack like denial-of-service (DoS), for example, jamming or power exhaustion. The defence system normally uses cryptography mechanisms to prevent or eliminate outsiders from joining the network. These techniques, however, are not effective when protecting against insider threats. Insider malicious nodes can be created by several ways: attackers physically capture the nodes and reprogram them, attackers use software and devices to breach the cryptography key or inject malicious code (?). On those cases, the attackers have all the keys, so they can easily overcome any cryptography test. The insider attacks usually aim at destroying a network operation so it is better to detect them by a well specified monitor system, which can discover early any anomaly network behaviour.

The outsider and insider attacks are applied on all layers of WSN. Some of these threats are more dangerous because they can easily be deployed and can generate complicated attacks. If the system cannot identify them early, their effects on network operation may be very serious both in short-term and long-term. One example is the Sybil attack, which uses the packet forging mechanism and leads to multiple other attacks like misdirection, exhaustion and unfairness (?). It will make the WSN unavailable, partitioned or resource exhausted. Another dangerous attack is the Sinkhole, which uses a packet dropping mechanism to attract traffic to a specific node. It generates selective forwarding, black hole attack and combines to partition the network (?).

Security threats from the internet side

End-users from the Internet can access information from the sensor field once 6LoWPAN is imple- mented. This raises the threats of authenticating from users and sensor motes, sensor network availability and user accountability. The adversary can access the information illegally if no authen- tication mechanism is applied in the network. When a communication channel between end-user and sensor network is established, the attacker can also eavesdrop on the sensitive information from the data stream, which breaks the network integrity. Besides that, the accountability of the users accessing the sensor network should be considered for detecting and recreating security incidents (?). The availability of the communication should be guaranteed by protecting the sensor side and adapting the operation of the Internet side with the resource constraint of the 802.15.4 nature.

Another type of threat is that an attacker from the Internet can get control of the sensor nodes. For example, the botnet attack creates a botnet inside the sensor network for forging the data collection sending to the sink. This attack falsifies the data in the user-end, which leads to wrong alarm or decision. The sensor botnet does not have enough resources for making a successful distributed DoS attack to other networks; however, attackers can make a distributed DoS attack to the botnet itself by flooding to drain the power source.

A cryptography line cannot defend against DoS attack from the Internet to the sensor network, so there is a need for implementing the IDS for analysing the IP traffic between the two. Besides that, traditional IDS solutions in the Internet or in the sensor network cannot be simply applied because of the dissimilarity of traffic pattern in these two network designs.

Security threats from the routing protocol for low-power and lossy network

The RPL is an underlying and specific routing protocol designed for the purpose of optimising 6LoWPAN operation. There are security mechanisms proposed for RPL but they only aim at pro- tecting it from external threats by control messages encrypting countermeasures. The drawbacks of 6LoWPAN security, such as weak communication link and nontampering nodes, make RPL weak from internal attack. Once a benign node becomes an internal adversary, it can break the network operation without being detected by cryptography mechanisms. Therefore, analysing RPL threats in addition to specifying its operation will help to monitor most of the internal malicious behaviours.

Current RPL threats directly attack the routing operation by changing the route, making it longer or even changing the destination address so that the time waiting for a packet goes to indefinite. Threats on other layers that aim at resource consuming such as flooding and overwhelming, or destroying network traffic like jamming or congestion can also be considered indirect attacks to the routing part because they downgrade the node operation. RPL is also vulnerable from passive eaves- dropping attacks and active tampering. The passive eavesdropping attacks can be prevented by using a symmetric key to encrypt the packets as proposed in. Tampering active nodes, however, creates compromised nodes, which can cooperate to break the protocol operation rules and easily overcome the cryptography line.

Besides that, RPL utilizes some specific rules for optimising network operation; nevertheless, adversaries can exploit these to create different attacks. Potential attacks of this kind are Rank, local repair and resource depletion attack.

Rank attacks. One kind of cooperated threat is the Rank attack. The RPL routing rule states that ‘rank strictly increases in the downstream direction and strictly decreases in the upstream direction’ [15]. This rule is created to prevent the nodes from creating unoptimised path or loop path. Consider a scenario when the source node 1 sends the packet to the destination node N through inter- mediate nodes 2,3,4,:::,N □ 1. Assume the rank of these N nodes are R_1,R_2,R_3,:::,$R_{n□}$,R_n consequently. The rank rule states that if node 1 sends packets upward to node N then the con- dition $R_1 > R_2 > R_3 >$: : :$R_{n□} > R_n$ must be satisfied; or if the route is downward then R_1 6 R_2 6 R_3 6 : : :$R_{n□}$ 6 R_n must be satisfied. The senders and receivers along the route have the responsibility to check these conditions and inform any breaking of this rule by setting the Rank-Error bit in the RPL Packet Information (?).

The RPL creates node rank as its unique parameter for easily choosing and maintaining the optimised path. The RPL requires all the nodes to check and follow this rule; however, its mechanism cannot protect against attacks from cooperated malicious node behaviours. The rank attack is easy to be implemented by simply skipping the rank checking function in the compromised nodes, or even injecting some code that breaks this function in the normal nodes. It is also difficult to be revealed because it does not need to spoof anything and most of the behaviours of the compromised nodes look like normal from their neighbours’ point of view. Once the rank rule is broken, the consequence can be (i) unoptimised path is created; (ii) if the attack is initiated in the route discovery phase, some optimised paths may be disrupted, which mean they exist but will never be discovered; and (iii) a loop can be created without any detection. These consequences definitely downgrade the network operation in many important aspects, such as throughput and delay.

Figure 4 below shows how the Rank attack creates an unoptimised path or a loop. In Figure 4(a), the two nodes 2 and 5 are compromised by the Rank attack and misdirect the packets from source 1 to destination 4 to the route 1–2–5–6–4 instead of the optimal route 1–2–3–4. The Rank rule is broken at the link 2–5, for example, by not setting the Rank-Error bit up. This scenario breaks the optimal topology and creates more delay to the route. In Figure 4(b), the four nodes 4, 5, 6, 7 are compro- mised by the Rank attack to direct the packets into the loop 1–2–3–4–5–6–7. The Rank attack in this scenario is more dangerous because it creates more delay, packet dropping and adds more workload to the nodes along the route. In both scenarios, the Rank rule is only broken at the link between the malicious nodes so it is difficult for other normal nodes to detect these anomaly behaviours.

Local repair attack. A node in RPL can start the local repair progress in two ways. The first way is the poisoning mechanism by changing its rank to infinitive and broadcast this rank to all of its neighbours. Those neighbours once receiving and updating the rank information of that node

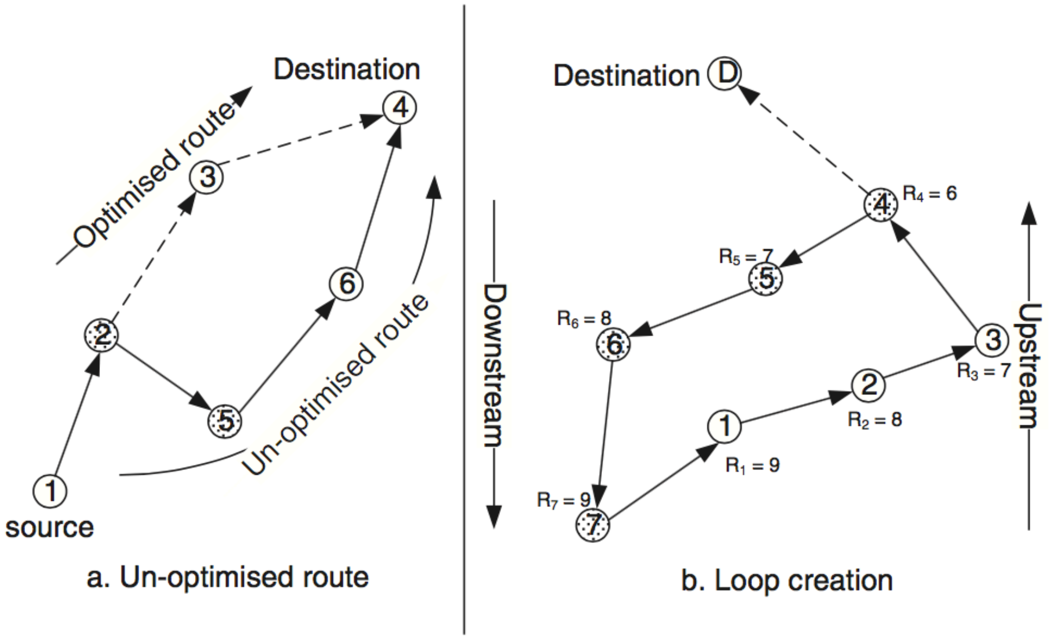


Figure 4. Unoptimised route and loop creation in rank attack scenario.

may need to find a new parent towards the root. The second way to do local repair is to change the DODAG ID value of the node. This metric is unique to each DODAG and shows what 6LoWPAN the node belongs to. A node changes its DODAG ID meaning that it left that DODAG and now belongs to a new DODAG neighbor (Just learn this in the class..interesting!). As a result, all of its child nodes need to do a local repair to find a new preferred parent.

In RPL, the node is supposed to only do local repair if the links towards its parent list are all broken. However, the adversary can make the node change its DODAG ID or broadcast infinitive rank frequently without any reason. Only the node itself can verify if the link to its preferred parent is broken or not, so when the other neighbors look at a frequent local repair made by a node, they cannot justify whether that node is benign or not.

Every time a local repair happens, the network topology will need to be updated. This will cost resources and degrade network operation. In case of changing DODAG ID, it is even worse because moving in and moving out a 6LoWPAN can create local repair in at least two DODAG.

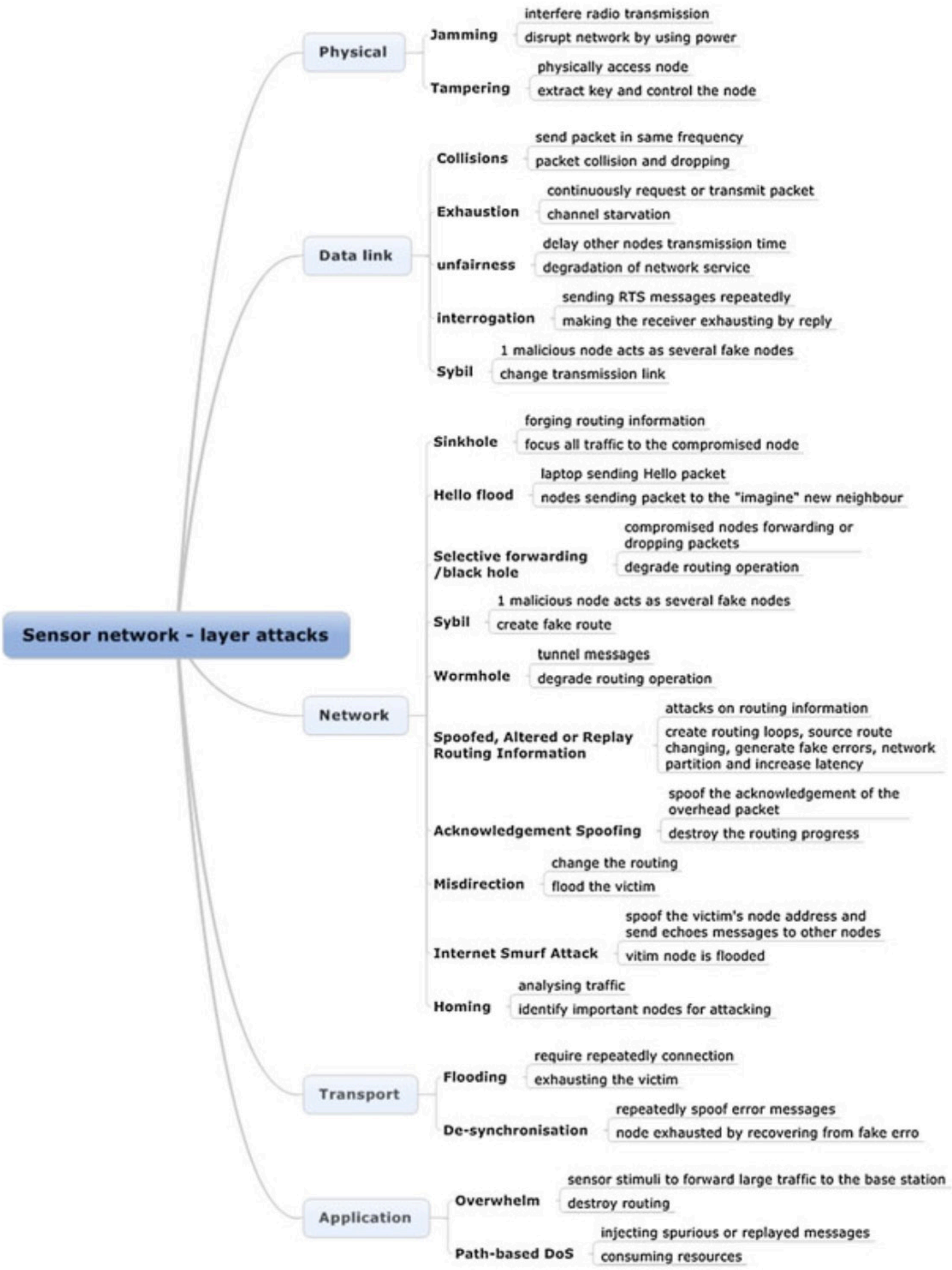

Sensor network - layer attacks
Physical
Jamming
interfere radio transmission
disrupt network by using power
Tampering
physically access node
extract key and control the node
Data link
Collisions
send packet in same frequency
packet collision and dropping
Exhaustion
continuously request or transmit packet
channel starvation
unfairness
delay other nodes transmission time
degradation of network service
interrogation
sending RTS messages repeatedly
making the receiver exhausting by reply
Sybil
1 malicious node acts as several fake nodes
change transmission link
Network
Sinkhole
forging routing information
focus all traffic to the compromised node
Hello flood
laptop sending Hello packet
nodes sending packet to the "imagine" new neighbour
Selective forwarding /black hole
compromised nodes forwarding or dropping packets
degrade routing operation
Sybil
1 malicious node acts as several fake nodes
create fake route
Wormhole
tunnel messages
degrade routing operation
Spoofed, Altered or Replay Routing Information
attacks on routing information
create routing loops, source route changing, generate fake errors, network partition and increase latency
Acknowledgement Spoofing
spoof the acknowledgement of the overhead packet
destroy the routing progress
Misdirection
change the routing
flood the victim
Internet Smurf Attack
spoof the victim's node address and send echoes messages to other nodes
vitim node is flooded
Homing
analysing traffic
identify important nodes for attacking
Transport
Flooding
require repeatedly connection
exhausting the victim
De-synchronisation
repeatedly spoof error messages
node exhausted by recovering from fake erro
Application
Overwhelm
sensor stimuli to forward large traffic to the base station
destroy routing
Path-based DoS
injecting spurious or replayed messages
consuming resources

Figure 3. Security threats from WSN side.

IEEE 802.15.4

In this section, I briefly discuss the IEEE 802.15.4 standard. The original IEEE 802.15.4 standard was released in 2003. The original version supported two physical layers, one of them working in the 868 and 915 MHz frequency bands and the other working in the 2.4GHz band. Later on, there was another revision released in 2006, which improved the transfer speeds. Additional bands were added in the subsequent revisions.

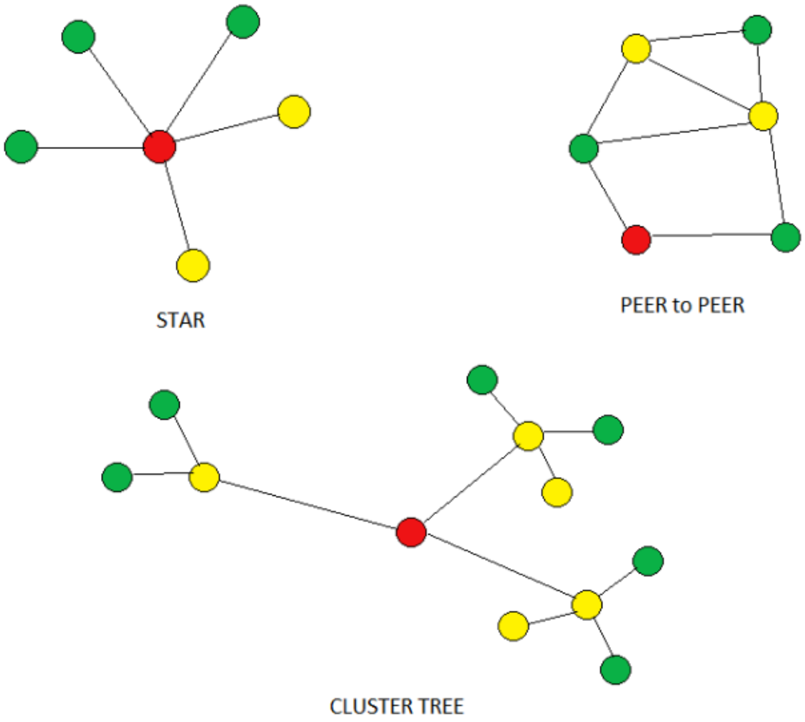


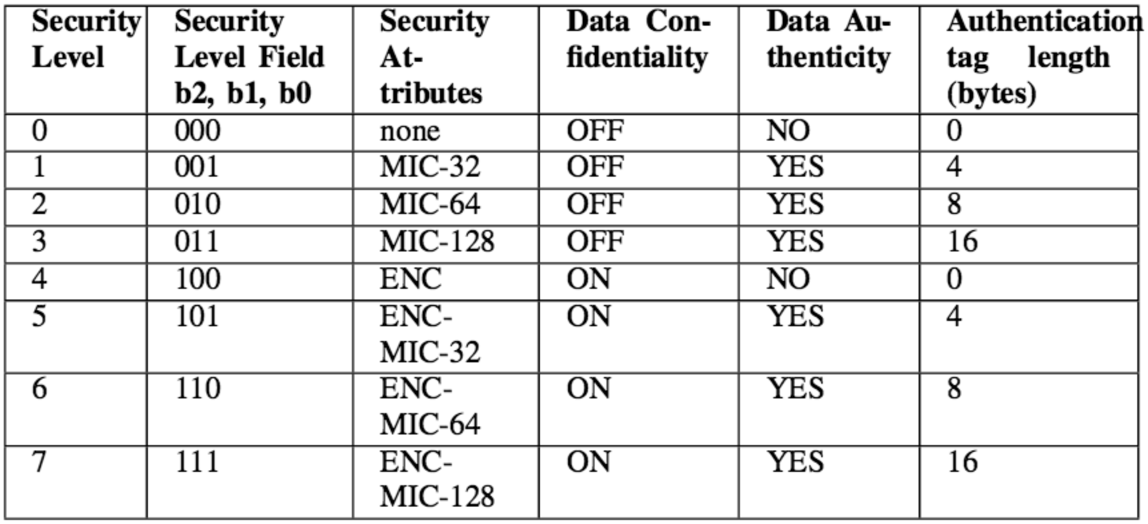
Fig. 1. Network Topologies

The IEEE 802.15.4 supports two classes of devices: Fully functional devices (FFD), which have full network functionalities and the Reduced functional devices (RFD), which possess limited functionalities. All personal area networks (PAN) consists of at least one FFD which acts as the PAN coordinator which is responsible for maintaining the PAN. RFDs are responsible for directly obtaining data from the environment and sending them to a PAN coordinator. Figure 1 shows the various topologies which a PAN can adopt. In the figure, the red devices are PAN coordinators, the yellow devices are FFDs but are not PAN coordinators and the green devices are RFDs. As seen from the figure, in a star topology, all devices directly interact with only the PAN coordinator. In a peer-to-peer topology, the FFDs can communicate with each other.

In a cluster tree topology, the RFDs communicate with an FFD which in turn communicate with the PAN coordinator. c2014, S.Sciancalepore, G.Piro, G.Boggia and L.A. Grieco3 been exchanged between two authorized node, may be stored and sent again into the network by a fraudulent device (i.e.,the so called replay attack). To prevent this kind of attack, the sender typically assigns a monotonically increasing sequence number to each packet and the receiver rejects packets with smaller sequence numbers than it has already seen. To offer these security services, the IEEE 802.15.4 specification introduces procedures and mechanisms for protecting MAC frames, through symmetric-key cryptography techniques based on the AES-CCM* algorithm. In the case security features are supported by a given device, the macSecurityEnabled attribute, stored at the MAC layer, is set to TRUE.

Security levels:
Eight security levels are defined to protect the frame generated at the MAC layer in different manners. As summarized in Tab. I below, they include unsecured, only encrypted, only authenticated, and encryption with authentication configurations. When the unsecured level is enabled, nor data confidentiality neither message integrity are provided. In other cases, instead, the data encryption and the authentication of messages are provided by means of AES and AES-CBC techniques, respectively. It is possible to offer a specific service to each kind of packet. However, the selection of the security level and the definition of other parameters required for performing security procedures have to be handled by an upper layer and then communicated to the MAC entity through dedicated primitives

TABLE I. DIFFERENT SECURITY LEVELS PROVIDED BY THE IEEE802.15.4 STANDARD



Security Level	**Security Level Field b2, b1, b0**	**Security Attributes**	**Data Confidentiality**	**Data Authenticity**	**Authentication tag length (bytes)**
0	000	none	OFF	NO	0
1	001	MIC-32	OFF	YES	4
2	010	MIC-64	OFF	YES	8
3	011	MIC-128	OFF	YES	16
4	100	ENC	ON	NO	0
5	101	ENC-MIC-32	ON	YES	4
6	110	ENC-MIC-64	ON	YES	8
7	111	ENC-MIC-128	ON	YES	16

IEEE 802.15.4 header structure:
The IEEE 802.15.4
MAC frame, which has been pictured in Fig 2 below, is composed by a MAC header, a payload and a Frame Check Sequence (FCS) footer. Security parameters are included within the Frame

Control and the Auxiliary Security Control fields. If the Security Enabled flag of the Frame Control field is set to 1, it means that the current MAC frame is protected and the node transmitting the packet supports at least one of the security services discussed above. If the flag is set to 0, instead, it means that the device sending the packet does not support any security capabilities and, for this reason, it is not able to send and receive encrypted and/or authenticated messages.

The Auxiliary Security Controlfield, which is present into the MAC header only if the Security Enabled flag is equal to 1, stores some parameters adopted for protecting the frame. They will be exploited by the destination node for performing the reverse security procedure (i.e, decryption and/or integrity check). This security header is composed by the Security Control, the Frame Counter, and the Key Identifier fields. The first one explains the security level and the key identification mode chosen by the sender. The counter stored into the second field is generated by the source in order to protect the message from replay attacks. Finally, the last field, i.e., the Key Identifier, is optional and it stores information (KeySource and KeyIndex) needed to determine the key exploited for the encryption of the message.

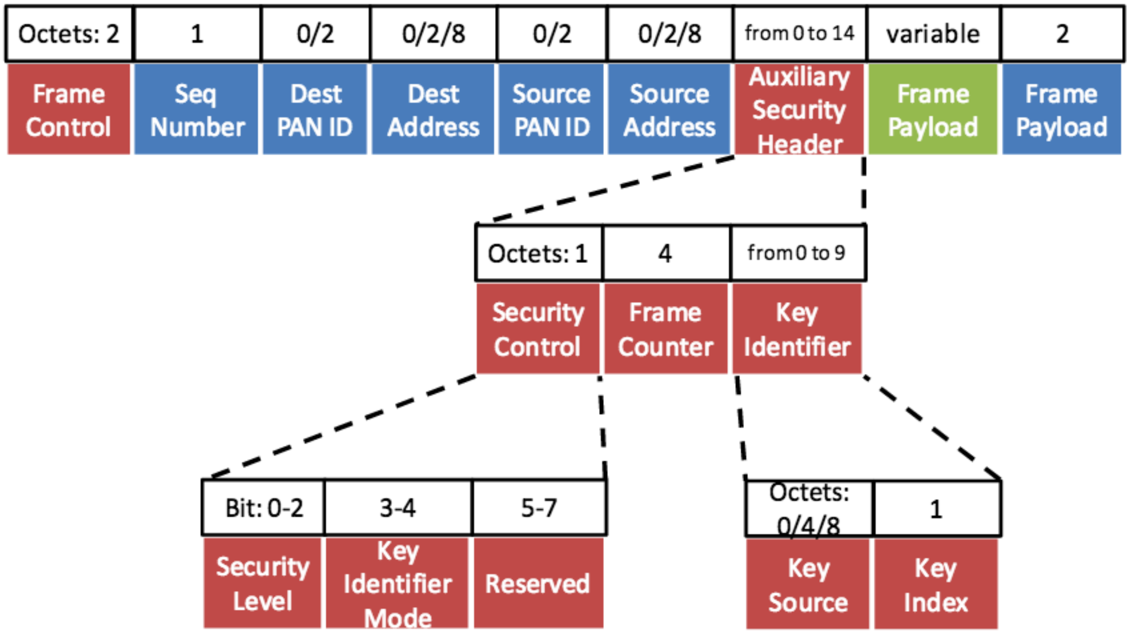


Fig. 2. The Auxiliary Security Header Structure

Security procedures and MAC PIB attributes:

At the MAC layer, encryption and decryption functionalities are implemented within the outgoing frame security and the incoming frame security procedures, respectively. It is very important to remark that the standard allows the possibility to use a dedicated key for each remote device and for each type of MAC frame (i.e., beacon, command frame, data packet, and

ACK). Moreover, it is necessary to define a specific security service to be guaranteed for each kind ofmessage. The related information is stored in the macSecurityLevelTable. It is composed by a set ofSecurityLevelDescriptor elements, which provide information about the frame type which it refers to, the minimal expected/required security level, the set of allowed security levels, and a boolean flag indicating if the minimal security service may be overridden by a given device. A node stores into the macDeviceTable the list of devices with which it can setup a secure communication. For each of them, a dedicated DeviceDescriptor is created. It contains the PAN ID, its short MAC address, its extended MAC addresses, as well as the counter of the latest packet received from the remote device and a boolean flag indicating if the considered node may override the minimum security level settings. Without any doubts, the most important attribute is the macKeyTable where all the keys are organized in. A keyDescriptor, i.e., the single element of the aforementioned table, contains the key, the set of devices that can use it, a list ofKeyUsageDescriptor indicating which frame may be protected with this key, and other parameters (e.g.,KeySource, keyIndex) used for uniquely identifying the key

Embedded Security

Embedded security means building security in from the start i.e. security features built into a device. Some of the major building blocks for embedded security for IoT is listed belo (?):

1. Cryptographic Algorithms: These are basically the

All solutions discussed basically focus on to speed up the basic security functions and it does not provide solutions against the majority of the security attacks. So, there is a need for an embedded security framework and architecture which will move security considerations from a function-centric perspective to system architecture (HW-SW) design issue.

BUILDING BLOCKS

Embedded security means building security in from the start i.e. security features built into a device. Some of the major building blocks for embedded security for IoT is listed below (?):

Side-channel HW-attack SW-attack Energy Efficiency Flexible Computational time cost essential building block of a robust security solution. The unusual design constraints placed on embedded devices require a new lightweight, highly efficient, easy to deploy cryptography scheme that provides high levels of security while minimizing memory, execution speed requirements and power requirements. Elliptic-Curve-Cryptography (ECC) is an essential methodology for meeting these requirements of embedded designs and that is the reason why it is essential for embedded security.

2. Secure Storage: Cryptographic algorithms require keys as their basis for operation. Since the algorithms are published and known to all, including to potential attackers, protecting the secrecy of the key is an important issue for security. Secure Storage essentially deals with protecting access to keys and other pieces of data. Secure Storage also needs to be persistent, such that items are not lost during power cycles. Examples of persistent storage are on-chip ROM memory, on- chip One-Time-Programmable (OTP) technology, as well as off-chip flash

memory.

3. Secure Boot : The purpose of Secure Boot is to bring the system to a known and trusted state. The Secure Boot routine is a ROM-based routine, so that an attacker cannot intercept the procedure. Additional features are required in order to provide a complete Secure Boot solution. These include the ability for software update at any point in time i.e a Software Version Revocation mechanism for system advancement to a new version of the software image with prevention of roll- back to an older version is a must.

Secure JTAG : The JTAG interface is a debugging interface for chips. It is used primarily during development and manufacturing, but also used to help debug errors that are found in the course of the lifetime of the system. The JTAG interface is potentially exploitable by attackers, who can try to read internal registers or memories.

5. Secure Execution Environment (SEE) : It refers to a processing unit which is capable of executing applications in a protected manner. The building blocks of an SEE are : a secure processor (either a dedicated processor or one capable of supporting a secure mode) which is hardware compartmentalized from the non-secure mode, Secure code and Data memory (most likely dedicated on-chip RAMs) and a Secure kernel for providing the interface between hardware and software.