**CYBER RISKS IN**

**INTERNET OF THINGS**

***A review report submitted for the course***

**Cyber security**

**CSE4003**

**Embedded Project**

WINTER SEMESTER 2017-18

**A2+TA2 SLOT**

**Review-III**

Submitted by:

|  |  |
| --- | --- |
| **Name** | **Reg. No.** |
|  |  |
| HEMANTH GRANDHI | 15BCB0027 |
|  |  |
| DIVYA DEBASHRITA | 15BCE0525 |
|  |  |
| VAISHALI YEGI | 15BCE2085 |
|  |  |



**SCOPE, VIT VELLORE,**

**TAMIL NADU- 632 014**

1. **INTRODUCTION**

The term ―Internet of Things‖ has been rapidly gaining popularity. The devices involved connect wirelessly, interact with each other and create data. IoT devices has become more convenient than it was before. IoT devices are capable of co-operating with one another. The World of IoT includes a huge variety of devices that include smart phones, personal computers, PDAs, laptops, tablets, and other hand-held embedded devices. The IoT devices are based on cost-effective sensors and wireless communication systems to communicate with each other and transfer meaningful information to the centralized system. The information from IoT devices is further processed in the centralized system and delivered to the intended destinations. With the rapid growth of communication and internet technology, our daily routines are more concentrated on a fictional space of virtual world. Due to its increased pervasiveness there has been a significant increase in the number of attacks and threats on the IOT devices and services is increasing too. Cyber criminals are working on new techniques for getting through the security of established organizations, accessing everything from IP to individual customer information — they are doing this so that they can cause damage, disrupt sensitive data and steal intellectual property. Not only is the number of attackers increasing along with the growing network size but the tools available to potential attackers are also becoming more sophisticated, efficient and effective.Wireless communication networks are highly prone to security threats. The major applications of wireless communication networks are in military, business, healthcare, retail, and transportations. These systems use wired, cellular, or adhocnetworks. Therefore, for IoT to achieve fullest potential, it needs protection against threats and vulnerabilities. Unfortunately, the majority of these devices and applications are not designed to handle the security and privacy attacks and it increases a lot of security and privacy issues in the IoT networks such as confidentiality, authentication, data integrity, access control, secrecy, etc.This paper seeks to contribute to a better understanding of threats and their attributes (motivation and capabilities) originating from various intruders like organizations and intelligence. The process of identifying threats to systems and system vulnerabilities is necessary for specifying a robust, complete set of security requirements and also helps determine if the security solution is secure against malicious attacks.

1. **LITERATURE SURVEY**

The advent of the IoT-cloud combination has brought multiple benefits to the information technology (IT) industry that includes embedded security, cost reductions, improved uptime, and an increase in redundancy and flexibility.[1]Technology is a fundamental part of modern-day society, and as such, the security of and trust that we place in IT systems are a significant concern. This is particularly true given the plethora of attacks being launched that target organizations, governments, and society. The Internet of Things (IoT) is set to benefit society through a range of smart platforms and a pervasive coupling of digital, cyber-physical, and social systems. [7] Security challenge is the main factor that affects the success of IoT. There should be some smart security solution to meet these crucial security challenges.

Millions of devices are connected through internet. So it would be difficult to identify if any unauthorized device connect with an existing network and steal the confidential and most import information during exchange over the internet. [2]The corporate business systems are assessed

primarily for the security risks to the confidentiality of information they process, with consideration of risks to integrity and availability frequently neglected. [3] Most of the problems in Internet of Things belong with wireless sensor connection issues and important confidentiality problems with Big Data.

1. Today’s computer systems must not be only preserve privacy of the data or messages but also the other factors like availability, integrity, non-repudiation etc. Blind dependency over wearable devices is also risky and sometimes leads with security problems. Companies, those who use IoT technique, need to find a way to store, track, analyze and make sense of the large amounts of data that will be generated.

Few security techniques of IoT are necessary to implement to protect your confidential and important data as well for the purpose of device protection through some internet security threats. To improve security, an IoT device that needs to be directly accessible over the Internet, should be segmented into its own network and have network access restricted. The network segment should then be monitored to identify potential anomalous traffic, and action should be taken if there is a problemBasic security mechanism includes providing username and password to the authorized user; and using that information to authenticate the user. [4] Unfortunately, the majority of these devices and applications are not designed to handle the security and privacy attacks and it increases a lot of security and privacy issues in the IoT networks such as confidentiality, authentication, data integrity, access control, secrecy, etc. [5].

**III.** **PROPOSED WORK**

We are going to analyze the threats at these different aspects of IOT:

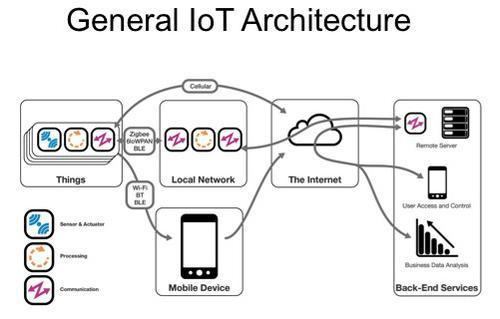
1. The device itself: It needs to be secure at the firmware level and even on the hardware side if the application is critical.
2. The infrastructure: Older platforms could have obsolete trust models and protocols, designed when we didn’t have these many connected ―things‖. A broken IoT devicecould be used to exploit this trust model and escalate the attack on the entire network.
3. The protocols: Many IoT devices need to run on long-lasting battery power, therefore state of the art protocols (e.g. TLS/SSL) could be too heavy for the deviceand must be left behind. In this case a secure perimeter could save a lot of time andeffort: like the usage of 4G protocols that cut through the local area network andoffset everything on the inherently secure cellular networks. Unfortunately cellularnetworks need operative expenses, require KYC (know your customer) and suffercountry-based restrictions or contracts.
4. Moore’s law: More computing power means that good encryption protocolstoday will be vulnerable in the future. Legacy methods could be unsafe in the future:Replacing millions of vulnerable devices which are hard-wired on old and brokenstandards.
5. The process: Every device has a lifecycle that needs to be secure. In many physicalapplications the installation should be done by trained workers (e.g. an electrician)instead of skilled security professionals. This is true also for password recovery, firmware update, device fixing. A lot of value could be unlocked by systemintegrators.

We will then take the following aspects into account, and taking into some practical real life scenarios, then come up with possible solutions to better the security status of IoT devices. These solutions should hold as a guide line while the development of new devices and these issues should be

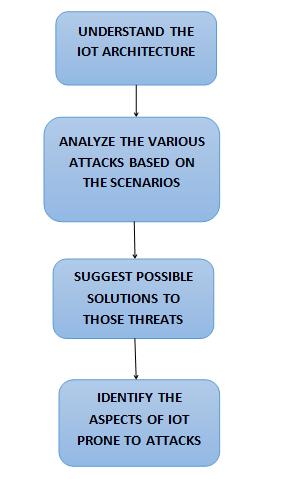
taken care of while implementing the projects, with this the known security issues will be acknowledged and worked upon by the innovators.

**IV. WORKING MODEL/DESIGN**

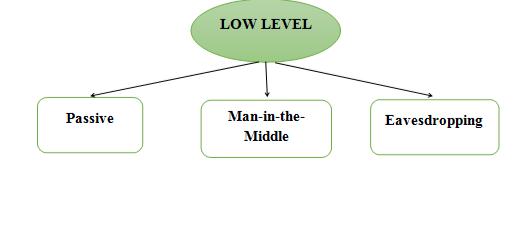
**A. ARCHITECTURE OF IOT:**

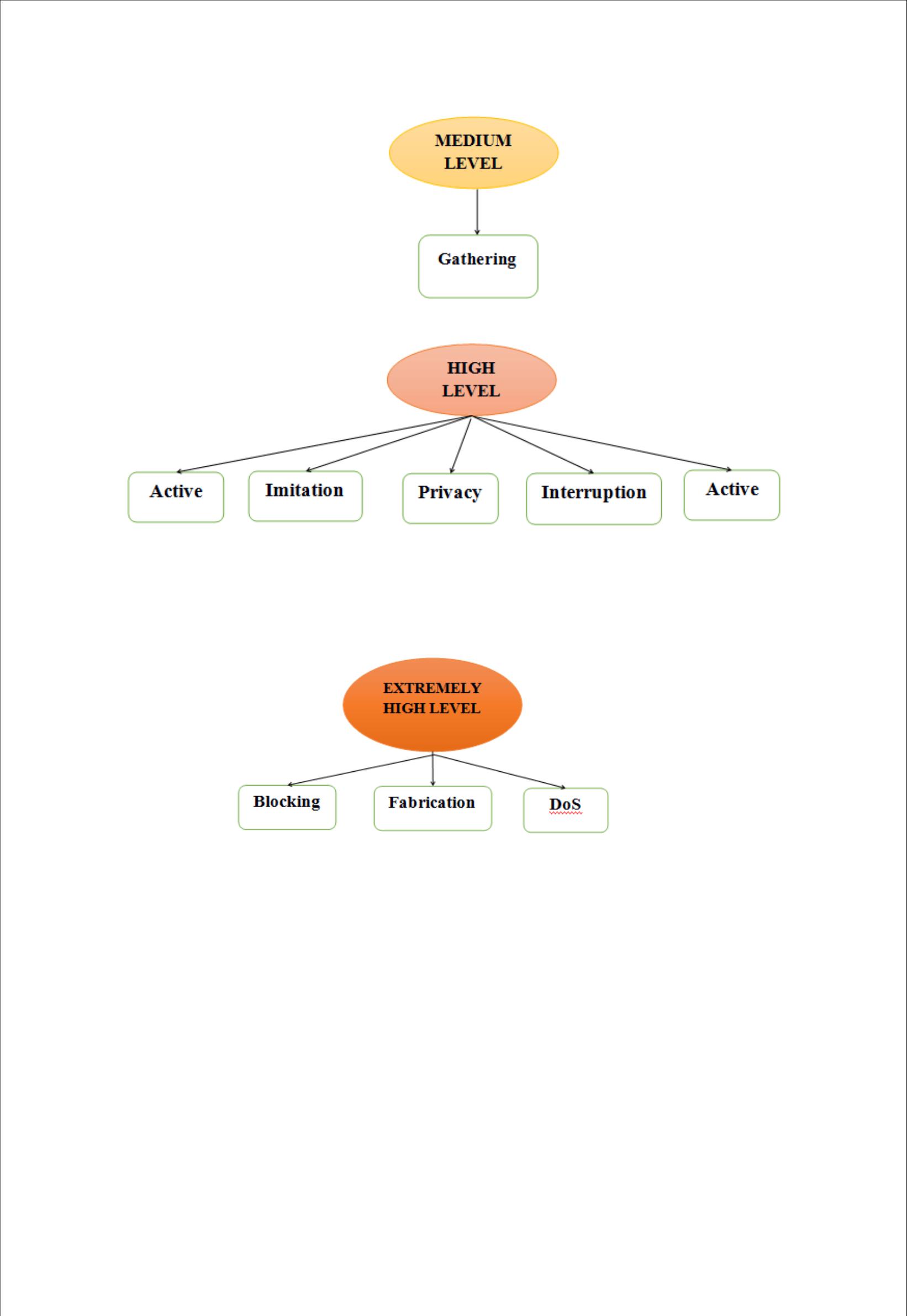
****

**B.** **WORKFLOW MODEL**

****

**C. DIFFERENT TYPES OF ATTACKS AND THEIR THREAT LEVELS, THEIR NATURE:**

****



**V. ANALYSIS OF DIFFERENT TYPES OF ATTACKS AND THEIR SOLUTIONS.**

**PROBLEMS WITH COMMUNICATION:**

The communication protocols available or being designed at the IEEE and IETF currently enable a standardized protocol. The mechanisms forming this stack must thus enable Internet communications involving constrained sensing devices, while copying with the requirements of low-energy communications environments and the goals and the lifetime of IoT applications. The diagram here shows all the protocols that are used at every level of the stack:

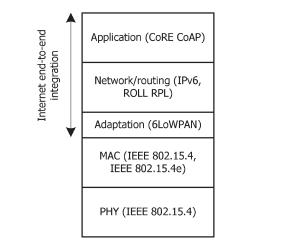


Fig1. The protocol stack

The coming sections discuss the problems associated and possible approaches for security to these stack layers.

**PART: 1 Security for the PHY and MAC layer**

The communications protocol stack for the IoT employs IEEE 802.15.4 with the goal of supporting low—energy communications at the physical (PHY) and Medium Access Control (MAC) layers.

**A. Security for IEEE 802.15.4**

Security as currently defined by IEEE 802.15.4 is optional, given that an

application may opt for no security or for security at others layers of the protocol stack.

Problems found were:

1. No specific keying structure is found. The reason is because the model is usually dependent on the threat model for that application and the resources (like sensing devices) to manage operations.
2. The IV values on ACL entries can pose a threat if the same key is used more than once, which is a high possibility among users, with reasons ranging from random selection to loss of ACL state due to power interruption to nodes waking up from low power mode. It can be dangerous with stream ciphers encrypting in the CRT mode as AES/CCM, as it may enable an attacker to recover plaintexts from cipher texts.
3. Tables storing ACL entries in IEEE 802.15.4 may not provide support for all keying models; mainly group keying and network-shared keying. Group keying is difficult to implement. The support of group keying requires various ACL entries using the same key, again promoting nonce reuse and the breaking of confidentiality. On the other end, network shared keying is incompatible with replay protection.

1. Currently, IEEE 802.15.4 is unable to protect acknowledgment messages in respect to integrity or confidentiality. An attacker may therefore forge acknowledgments and perform DoS attacks.

**SOLUTION:** In IEEE 802.15.4, the applications are responsible for the communication schedules, and security mechanisms can be proposed to take the advantage that the MAC layer operates using time-synchronized and channel-hopping communications. We can design schedules with slots reserved a priori for security, and that could manage operations like key management, identifying misbehaving nodes for intrusion detection. Security solutions for IPv6 over TCSH mode can be formulated.

**PART 2: (Security for network layer)**

**Problems and threats:**

1. Security threat over 6LoWPAN: Neighbor Discovery and mesh routing mechanisms on IEEE 802.15.4 environments may be susceptible to security threats, and AES security at the link-layer can provide a basis for the development of mechanisms protecting against such threats, particularly for very constrained devices. Other method could be employing more powerful 6LoWPAN devices in order to support heavy security related operations.
2. Discussions regarding RFC security: The focus here is on security issues posed by the usage of a mechanism inherited from RFC 4944, which enables the compression of a particular range of 16 UDP port numbers down to 4 bits. The overload of ports in this range, if employed with applications not honoring the reserved set for port compression, may increase the risk of an application getting the wrong type of payload or of an application misinterpreting the content of a message. Thus these have to be employed with a MAC security mechanism.

**SOLUTION:** There are several methods that can beused to ensure the security at network layer. For wireless networks, using Wireless Protected Access 2 (WPA2) instead of Wireless Encryption Protocol (WEP) can make the network use stronger complex wireless encryption. Also, for these networks, it is recommended to use several Service Set Identifiers (SSID), rather than just one. Hence, we can have different policies through each segment and assign each for different case of threat. As a result, if any segment gets attacked, other segments will stay safe.

On the other hand, using PPSK (Private Pre-Shared Key) for each sensor or device connected to the network. By providing different uniques keys, the access domain for each type of device can be defined easily. Also, disabling guest and default passwords in network devices such as routers and gateways should be done immediately upon unpacking a new network device.

**PART 3: Security in Routing**

The Routing Over Low-power and Lossy Networks (ROLL) working group of the IETF was formed with the goal of designing routing solutions for IoT applications. RPL provides in reality a framework that is adaptable to the requirements of particular classes of applications.The adoption of appropriate routing strategies in 6LoWPAN environments is a very challenging task, mostly due to the inherent specificities of each application and of the constraints of the sensing devices employed. In consequence, RPL assumes that routing must adapt to the requirements of particular application areas and, for each application area, an appropriate RFC documents an objective function that maps the optimization requirements of the target scenario.Considering that in the most typical setting various LoWPANnodes are connected through multi-hop paths to a small set of root devices responsible for data collection and coordination,RPL builds a Destination Oriented Directed Acyclic Graph (DODAG) identified by a DODAGID for each root device, by accounting for link costs, node attributes, note status information, and its respective objective function.The current RPL specification recognizes the importance of supporting mechanisms to secure routing messages exchanged between sensing devices and, in consequence, RPL defines secure versions of the various routing control messages.

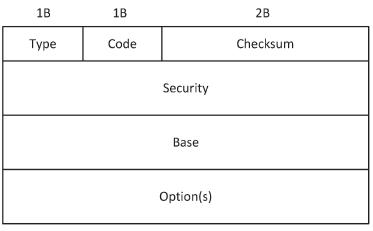


Fig2. Secure RPL control message

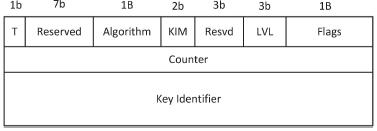


Fig3. Security part of the RPL control message

The RPL specification defines secure versions of the various routing control messages, as well as three basic security modes.The high order bit of the RPL Codefield identifies whether or not security is applied to a given RPL message. The information in the Security field indicates the level of security and the cryptographic algorithms employed

to process security for the message, the security transformation itself states how the cryptographic fields should be employed in the context of the protected message.The current RPL specification defines the employment of AES/CCM with 128-bit keys for MAC generation supporting integrity and of RSA with SHA-256 for digital signatures supporting integrity and data authenticity.The LVL (Security Level) field indicates the provided packet security and allows for varying levels of data authentication and, optionally, of data confidentiality.A Consistency Check (CC) control message enables a sensing node to issue a challenge-response with the goal ofvalidating another node’s current counter value. Semantic security and protection against packet replay attacks is provided with the help of the Counter field. The KIM (Key Identifier Mode) field of the Security section indicates whether the cryptographic key required to process security for this message may be determined implicitly or explicitly.RPL defines how security is applied to routing control messages, and the current specification also defines the following three security modes: Unsecured, Preinstalled, Authenticated. There is a necessity of handling such metrics in a secure and trustful manner, including protection against nodes being able to falsify or lie in the advertisement of metrics, as a way to protect against attacks on routing operations.

**PART 4: (security in application layer)**

Application-layer communications are supported by the CoAPprotocol. The CoAP protocol implements a set of techniques to compress application-layer protocol metadata without compromising application inter-operability, in conformance with the representational state transfer (REST) architecture of the web. CoAP is currently defined only for UDP communications over 6LoWPAN. Application-layer communications may enable IoT sensing applications to interoperate with existing Internet applications without requiring specialized application oriented code or translation mechanisms. The CoAP protocol provides a request and response communications model between application endpoints and enables the usage of key concepts of the web, namely the usage of URI addresses to identify the resources available on constrained sensing devices.



Fig4. Format of CoAP message header

Messages in the CoAP protocol are exchange asynchronously between two endpoints, and used to transport CoAP requests and responses. CoAP provides a lightweight reliability mechanism. Using this mechanism CoAP messages may be marked as Confirmable, for which the sender activates a simple stop-and-wait retransmission mechanism with exponential back-off. The receiver must acknowledge a Confirmable message with a corresponding Acknowledgemessage or, if it lacks context to process the

message properly, reject it with a Reset message.The CoAPmessage starts with a 4-byte fixed header, formed by the Version field (2 bits), the T (message type) field (2 bits), the TKL (Token Length) field (4 bits), the Code field (8 bits) and the Message ID (16 bits). The token in practice enables a CoAP entity to perform matching of CoAP requests and replies, while the message ID supports duplicate detection and optional reliability.The CoAP Protocol defines bindings to DTLS (Datagram Transport-Layer Security to secure CoAP messages. The adoption of DTLS implies that security is supported at the transport-layer, rather than being designed in the context of the application-layer protocol. DTLS provides guarantees in terms of confidentiality, integrity, authentication and non-repudiationfor application-layer communications using CoAP. Once the initial DTLS handshake is completed, DTLS adds a limited per-datagram overhead of 13 bytes.

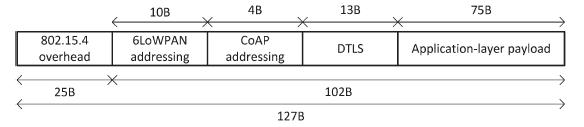


Fig5. payload space with DTLS on 6LoWPAN environments.

Security against replay attacks may also be achieved in the context of DTLS, using a different nonce value for each secured CoAP packet. In addition to the adoption of DTLS, CoAP currently defines four security modes that applicationsmay employ: NoSec(no Security), PreSharedKey(employed by sensing devices pre-programmed with cryptographic keys), RawPublicKey(authentication based onPubic Keys), Certificates( makes use of security certificates). An important aspect of CoAP security using DTLS is that Elliptic Curve Cryptography (ECC) [48] is adopted to support the RawPublicKeyand Certificates security modes. ECC supports device authentication using the Elliptic Curve Digital Signature Algorithm. The current CoAP specification defines a mandatory-to implement cipher suite for each security mode, based on the usage ofAES/CCMandECCcryptographic operations

**PART 5: Generalized Problems and Solutions**

The various attacks and threats which are possible because of the vulnerabilities available in the different communication protocol and existing mechanisms can be grouped as twelve different types. Each of the threats is important to address and certain measures are required to improve security:

1. **Passive:** This attack is a low level threat. It usuallydeals with a breach in dataconfidentiality. Examples are passive eavesdropping and traffic analysis. Hostile silently listen the communication for his own benefits without altering the data. We need to ensureconfidentiality of data and not allow an attacker to fetch information using symmetric encryption techniques.

1. **Man-in-the-Middle:** This attack is a low to medium level threat. It deals with theAlteration and eavesdropping are the examples of this attack. An eavesdropper can silently sense the transmission medium and can modify the data if encryption is not applied and steal the information that is being transmitted. Hostile may also manipulate the data. We need to apply data confidentiality and proper integration on data to ensure integrity. Encryption can be also applied so that no one can steal the information or modify the information or encode the information before transmission.
2. **Eavesdropping**: This threat is a low to medium level threat. In this threat,information content may be lost by an eavesdropper that silently senses the medium. For example in medical environment, privacy of a patient may be leaked. To counter this, we can apply encryption on all the devices that perform communication.
3. **Gathering:** This is a medium level threat. It occurs when data is gathered fromdifferent wireless or wired medium. Examples are skimming, tampering and eavesdropping. Data is being collected to detect messages. Messages may also be altered.Encryption can be applied to prevent this kind of attack. Identity based method and message authentication code can also be applied in order to prevent the network from such malicious attacks.
4. **Active:** This is a high level threat. It affects confidentiality and integrity of data.Hostile can alter the integrity of messages, block messages, or may re-route the messages. It could be an internal attacker. We should ensure both confidentiality and integrity of data. To maintaindata confidentiality, symmetric encryption can be applied. Anauthentication mechanism may be applied to allow data access to only authorized person.
5. **Imitation:** This is a high level threat. It is impersonating for an unauthorized access.Spoofing and cloning are the examples of this attack. In spoofing attack a malicious node impersonate any other device and launch attacks to steal data or to spread malware. Cloning can re-write or duplicate data.To avoid from spoofing and cloning attacks, apply identity based authentication protocols. Physically un-clonable function is a countermeasure for cloning attack.
6. **Privacy:** This is a high level threat. Sensitive information of an individual or groupmay be disclosed. Such attacks may be correlated to gathering attack or may cause an imitation attack that can further lead to exposure of privacy. In order to safe guard from this attack, we should apply anonymous data transmission. Transmit sample data instead of actual data. Can also apply techniques like ring signature and blind signature.
7. **Interruption:** This is a high level threat. It affects availability of data. This makesthe network unavailable.Applying authorization, only authorized users are allowed to access specific information to perform certain operation, helps handle this threat.
8. **Routing diversion:** where only the route increased. We need to diverted.

This is a High level threat. It is a simple yet dangerous threat is diverted showing the huge traffic and the response time hence ensure connectivity based approach so no route will be

* 1. **Blocking:** This is an extremely high level threat. It is a type of DoS, jamming, ormalware attacks. It sends huge streams of data which may lead to jamming of network, similarly different types of viruses like Trojan horses, worms, and other programs can disturb the network.We should turn on the firewall, apply packet filtering, anti-jamming, active jamming, and updated antivirus programs in order to protect the network from such attacks.

1. **Fabrication:** This is an extremely high level threat. It affects the authenticity ofinformation. Hostile can inject false data and can destroy the authenticity of information.Data authenticity can be applied to ensure that no information is changed during the transmission of data.
   1. **DoS:** This is an extremely high level attack. A malicious user may modify thepackets or resend a packet again and again on network. User can also send bulk messages to devices in order to disturb the normal functionalities of devices.We should apply cryptographic techniques to ensure security of network. Apply authenticity to detect the malicious user and block them permanently. In this way, the network is prevented from damage.

**REFERENCES**

* 1. J. R. C. Nurse, S. Creese and D. De Roure, "Security Risk Assessment in Internet of Things Systems," in IT Professional, vol. 19, no. 5, pp. 20-26, 2017.

1. J. C. Talwana and H. J. Hua, "Smart World of Internet of Things (IoT) and Its Security Concerns," 2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Chengdu, 2016.
2. M. StJohn-Green, R. Piggin, J. A. McDermid and R. Oates, "Combined security and safety risk assessment — What needs to be done for ICS and the IoT," 10th IET System Safety and Cyber-Security Conference 2015, Bristol, 2015
3. E. Bertino and W. Lafayette, ―Data Security and Privacy in the IoT,‖ pp. 18–

20, 2016.

1. S. Pilani, ―Handbook of Research on Modern Cryptographic Solutions for Computer and Cyber Security,‖ no. May, 2016.
2. A. Sajid, H. Abbas, and K. Saleem, ―Cloud-Assisted IoT-Based SCADA Systems Security : A Review of the State of the Art and Future Challenges,‖ vol. 4,

2016.

1. M. M. Hossain, M. Fotouhi, and R. Hasan, ―Towards an analysis of security issues, challenges, and open problems in the internet of things,‖ in Services

(SERVICES), 2015 IEEE World Congress on. IEEE, 2015, pp. 21–28.