NAME-SHANU KUMAR ,187159 ,SEC-A , IOT MINOR-1

SECURITY MECHANISM IN 6LOWPAN

INTRODUCTION

- The Internet of Things concept gained popularity in the last couple of years.With the emergence of internet of things (IoT), the physical object belonging to our daily activity and to different domain as: home automation, industrial automation, monitoring environment and health care may be interacted and benefited from the world of internet.
- Thus, this communication provides several data that are circulate in the different networks as IPv6 network or the 6LoWPAN network. Since the 6LoWPAN network is the fundamental part of IoT, Its security is challenge domain whether for the end-to-end security when the data are sent to the server outside the network or for the internal security with the intrusion detection system.
- In all these paper, we present a survey about the proposed researches for the 6LoWPAN network security mechanism and survey about,whether for inside or outside communication of network and related to 6LoWPAN.
- The analysis of these proposed security mechanisms is discussed based on a taxonomy focusing on the following attributes: the selected internet security protocols as DTLS, HIP and IKE for the end-to-end security (out-side the 6LoWPAN network) and the attack detected as routing attack, DDoS attack,…etc. for the intrusion detection system (inside the 6LoWPAN network). We also give the Evaluation of these security mechanisms for 6LoWPAN network in term of different metrics. The aim of this work is to identify leading trends, open issues, and future research possibilities
- The emergence of internet of things (IoT), the physical object belonging to our daily activity and to different domain as: home automation, industrial automation, monitoring environment and health care may be interacted and benefited from the world of internet. Thus, this communication provides several data that are circulate in the different networks as IPv6 network or the 6LoWPAN network.
- Since the 6LoWPAN network is the fundamental part of IoT, its security is challenge domain whether for the end-to-end security when the data are sent to the server outside the network or for the internal security with the intrusion detection system.

Why the topic is interesting .

- 6LoWPAN is the fundamental part of IOT , its security mechanism is very important part.The 6LoWPAN concept originated from the idea that "the Internet Protocol could and should be applied even to the smallest devices,".and that low-power devices with limited processing capabilities should be able to participate in the Internet of Things.That's why it is important to secure.

Paper-1:

Title:=A survey on Techniques for Securing 6LoWPAN

- The integration of low power wireless personal area networks (LoWPANs) with the Internet allows the vast number of smart objects to harvest data and information through the Internet.
- To provide security from both, along with Cryptography techniques, there also requires certain mechanism which provides anonymity & privacy to the communicating parties in the network in addition to providing Confidentiality & Integrity.
- . This paper provides survey on techniques used for securing 6LoWPAN from different attacks and aims to assist the researchers and application developers to provide baseline reference to further carry out their research in this field.

• Without an IP-based architecture, allowing communication of such constrained devices over the Internet require an application layer gateways, which are very complex to design and manage. Hence, the Internet Engineering Task Force (IETF) created Working Groups (WGs) called 6LoWPAN to standardize necessary adaptations of IPv6 for networks that use the IEEE 802.15.4 physical (PHY) layer, and has defined how to carry IPv6 datagrams over IEEE 802.15.4 links.

working model-6LoWPAN fulfils two primary elements: Header Compression: IPv6 header fields can be eliminated from a packet at network layer and derived from the link layer frames. Fragmentation: IPv6 minimum MTU requirement is 1280 bytes and IEEE 802.15.4 supports for 127 bytes . Hence to allow the cross-communication, fragmentation is done by 6LoWPAN Layer.

Advantages:-In some paper, specific methods are designed to defend against attacks like fragmentation & re-assembly buffer and botnet attack. Also, different IDS Solutions are combined to fulfil the security requirements of 6LoWPAN. More or less each technique has its specific advantages and limitations considering which it is used in various applications.MT6D is the only technique which provides security solution from both Internal as well as External attacks. Hence, making usage of such strong technique is recommended in 6LoWPAN.

COMPARISION OF PROPOSED TECHNIQUES:-

Operational Layer=>6LoWPAN Adaptation Layer

Security Properties	**Technique Description**
Confidentiality, Integrity and Authentication.	AH and ESP Header Compression using NHC Encoding for IPv6 Extension headers.
Protection of Shared Keys.	Automatic key exchange protocol based on ECC and Diffie Hellmann for use with Compressed IPsec.
Protection against Fragmentation replay attacks.	Addition of Timestamp and Nonce at each fragment for unidirectional & bidirectional packets
Protection against Fragmentation and Buffer Reservation Attack.	Addition of hashed value at the end of each fragment. Splitting the Buffer into slots to set the limit for an attacker
Protection against Botnet Attack.	Adding the Bot Detection Module to detect the malicious traffic in the network.
Protection against Internal/DOS attack.	Combined IDS Solution for detecting different network's traffic patterns.
Privacy & Anonymity	Rotating nodes addresses frequently to limit the attacker's time to track the address.

Paper-2:

Title:-6LoWPAN multi-layered security protocol based on IEEE 802.15.4 security features

In this paper,New multilayer security protocol based on the security specifications of the IEEE 802.15.4 standard, operating at both the MAC and the 6LoWPAN adaptation layers in order to ensure all essential security aspects to broad public and industrial acceptance.
The paper organized as follows,
1.Describes the state of the art 6LoWPAN security solutions.
End-To-End security:provide the benefit of enabling secure communications between IPv6 enabled sensor networks and the Internet.
Hop-By-Hop security:provides hop by hop secure communication between neighboring sensors in order to cover all links resilience.
6LoWPAN Routing::Routing schema in 6LoWPAN networks.which are e mesh under and route over schema.
2.This highlight different 6LoWPAN security attacks.
Hop-by-hop attacks:. Threats affecting physical links, radio hops and routing discovery, give rise to malfunction and resources exhausting. Jamming attack disrupts nodes' signal by increasing its power spectral density
End-to-end attacks: End devices perform packet fragmentation and reassembly in IPv6, thus end-to-end security is indispensable to prevent modifying or rebuilding packet fragmentation.
3.. An elaborated description of the our security protocol and algorithm.
Algorithm 1 Combined 6LoWPSec:- By activating the SecurityEnabled field and by setting the SecurityLevel field greater than zero, the security features of the IEEE 802.15.4 security sublayer will be carried out to achieve data protection between the different 6LowPAN entities.First, it enables separately the HbHSecEnabled by setting the macSecurityEnabled field to 1 as well as the E2ESecEnabled when setting the reserved field of the FrameControl to 1. Subsequently, our proposed protocol will operate alternately between the adaptation and the MAC layers respecting two security times: E2ESecT and HbHSecT.
4. Discussed the performance of our protocol in terms of energy consumption, packet delivery ratio, end-to-end delay, and security overhead.
Testbed platform and experimental setup:-COOJA network simulator for Contiki OS to analyze performance of 6LoWPSec.The deployment of such protocol requires the modification of the existing Contiki rime stack, that accommodate mesh-under routing, to support LOADng routing protocol with respect to and also to promote the use of IEEE 802.15.4 MAC security specifications at both the MAC and the adaptation layers.
Analyze memory allocation:- Focused on the impact of our proposed security protocol on memory consumption for different security levels and MIC sizes.

Combined 6LoWPSec Mode	Border Router	6LoWPAN mote
Nullsec	40.48KB	39.97KB
MIC-32	41.38KB	40.21KB
MIC-64	41.92 KB	41.21KB
MIC-128	42.22 KB	41.61 KB
ENC	40.93 KB	40.11KB
ENC-MIC-32	42.08 KB	41.58 KB
ENC-MIC-64	42.77 KB	42.38 KB
ENC-MIC-128	43.21 KB	42.73 KB

Analyze energy consumption:-To keep the trade-off between providing security functionality and limiting energy consumption, it is essential to maintain the security configuration.Measurements are captured during a period of 30 min for different scenarios in the presence and the absence of attack.
End-to-End delay:-Time taken for a packet to reach across a network from source to destination.Favoring of the E2E security generates a proper functioning of the entire network while alternating with hopby-hop security prevents the appearance of intruder nodes inside the LoWPAN.

Paper-3

Title:-Design of Embedded Secure Gateway Based on 6LoWPAN

-The paper proposes an embedded security gateway based on 6LoWPAN, which connects wireless sensor network with IPv6 network.The experimental results show that the design of gateway can realize communication authentication and security between the gateway and sensor node, and it balances performance and security.
-This paper proposes an embedded secure gateway based on 6LoWPAN, by combining the proxy architecture and the TCP/IP interconnection. The gateway achieves direct communication between end users and sensor nodes, and enables users to query real-time sensor data and stored historical data. Besides, it introduces user verification mechanism and the SNEP protocol which implements communication security.
-Sensor nodes are generally deployed in open environment, and messages are easy to be attacked in transmission process. Although IEEE 802.15.4 provides AES (Advanced Encryption Standard) security, the mechanism is comparatively loose.So proposed an embedded gateway design based on the 6LoWPAN, which provides an efficient, secure and trustworthy communication infrastructure between IPv6 networks and WSN. The technical contributions are as follows.
1.Address mapping table in the gateway which provides mapping between 16-bit IEEE 802.15.4 addresses and 128-bit IPv6 addresses.
2. Gateway design adopts SPINS (security protocols for sensor networks), which includes SNEP (secure network encryption protocol) and μTESLA (micro timed efficient streaming loss-tolerant authentication protocol) to provide security in WSN communication.
3.A web server in the gateway, which stores data periodically collected from sensor nodes. Users are able to query stored historical data.
Paper has some section as follows:-
1.Reviews the related work on WSN-IP network interconnection:-
Three approaches:-
A- proxy architecture, a special proxy server is deployed between the sensor network and TCP/IP network.
B-DTN (Delay Tolerant Networks) overlays- Designed for fault-prone disturbed environment. DTN gateway forwards bundles between regions which share a common bundle layer that resides above the transport layer.
C-TCP/IP for sensor networks-allows seamless integration of the sensor network and TCP/IP network, without additional proxies or gateways.
2.Interprets the access system of 6LoWPAN network and functions of the gateway:-
Interconnection of WSN and IPv6 network.

Senser Network---->Gateway<----->Internet------>Users

First, an IP user connects to the gateway. Then, the gateway identifies the user, while only a legal user is permitted to submit query request about sensor nodes. Finally, the gateway

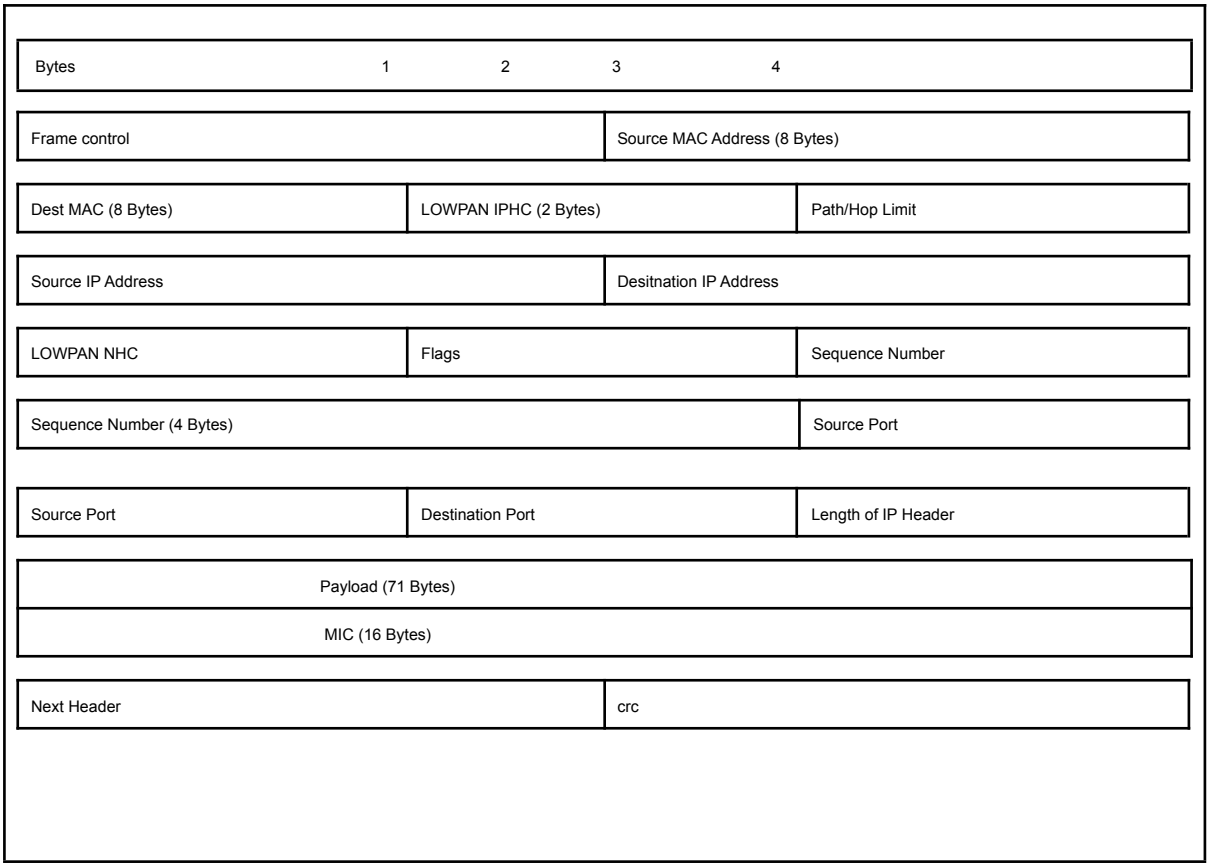
sends processed query information to the WSN, and subsequently replies results to query users.
3.Evaluates the performance of the gateway on NS2 simulation platform and analyzes experiment results-:NS2 (Network Simulator, version 2, [13]) to evaluate the performance is used of proposed gateway architecture.We use RC5 and CBC-MAC algorithms to implement encryption and authentication in SNEP.
SNEP Protocol:-The system adopts SNEP (secure network encryption protocol) to implement two-party authentication, data confidentiality, integrity as well as freshness. SNEP is a proprietary protocol of WSN with low communication overhead.
Security Management module(SMM):-consists of a security module and a data aggregation module.

Paper-4

Title:-Implementation of Secure 6LoWPAN Communications for Tactical Wireless Sensor Networks

- **The Paper** proposed the Tactical wireless sensor networks (WSN) consist of power constrained devices spread throughout a region of interest to provide data extraction in real time.
- In this paper we develop security mechanisms to be implemented on a tactical WSN using the 6LoWPAN protocol for use by the United States Marine Corps (USMC).
- we develop an architectural framework for tactical WSNs by studying security gaps and vulnerabilities within the 6LoWPAN security sublayer which is based on IEEE 802.15.4
- We develop a key management scheme that is non-broadcast but that is also feasible in an operational scenario.

The use of 6LoWPAN would significantly change the information flow as it currently exists by allowing multiple users in a unit to access sensor information despite their location.In this paper we propose a theoretical network design framework that uses 6LoWPAN and IEEE 802.15.4 such that it can be deployed for tactical operations by the Marine Corps
Paper organized as follows-:
1. Fundamentals of 6LoWPAN/IEEE 802.15.4-:To develop a cross layer load balancing/routing scheme for tactical WSNs.Encryption within the 6LoWPAN environment is a requirement in order to have an effective tactical WSN and it has been addressed in the most recent release of the IEEE 802.15.4 standard
2.comprehensive discussion on the theoretical tactical WSN framework, including network design and setup, 6LoWPAN packet structure and security mechanisms and planned simulation setup-:
A. Network Design-:The proposed network design includes multiple elements, each serving a specific purpose.As : master station (MS), base station/border router (BS), and sensor nodes.
B. Command and Control (Administrative Control)-:The control mechanisms of the MS include node control, defined routing, and keying mechanisms.
C. Encryption-: AES is used as the keying mechanism in this paper. The seven modes of AES boast different levels of encryption and authentication
D. 6LoWPAN Packet Structure-:: The proposed routing mechanism defined in this paper limits the direction each packet can take to reach the BS from the node.



E. Transition-:The transition of the packet from one domain to the other is to be completed by the Base Station (The BS is the transitional element within the WSN that connects the 6LoWPAN/internal environment to the public/external environment).
F. Deployment of Nodes-:Creating the network first requires setup of the key exchange for encryption purposes, the routing table to be loaded, and evaluation of ideal physical placements for the nodes.

Paper-5

Title-:A PMIPv6-based Secured Mobility Scheme for 6LoWPAN

-In this paper, a secure PMIPv6-based mobility scheme is designed. The proposed scheme enables a 6LoWPAN device to efficiently and securely roam in the 6LoWPAN networks.mobility management, a network based localized mobility management (NETLMM) protocol named Proxy Mobile IPv6 (PMIPv6) is proposed.
-The mobility of the users needs efficient mobility management to prevent the disconnection of the network. A host-based Mobile IPv6 (MIPv6) protocol has been proposed by the IETF for mobile nodes (MNs) to continuously access the network services while moving among foreign networks.
-FPMIPv6 performs better in term of packet loss compared to PMIPv6. However, more resources and larger buffer size of mobile access gateway (MAG) are required. To reduce the handover latency, a fast and localized PMIPv6 (FLPMIPv6) has been proposed
The paper organised as follows-:
1.SYSTEM BACKGROUND (system model)-:
A. System Architecture-:The system consists of a number of 6LoWPAN MNs (6MNs), some 6LoWPAN MAGs (6MAGs), a LMA and a remote authentication, authorization, and accounting (AAA) server.

B. Attack Model -: The threat model to PBSMS is based on the DolevYao intruder model .
2., the proposed scheme is described in details-:
A. Motivation-: The PBSMS scheme is designed to provide a more secure and efficient handover procedure for 6LoWPAN networks. The 6MN and the LMA will generate a shared keychain for secure communication.
B. Details of the Proposed Scheme :-The PBSMS is designed for secure mobility in 6LoWPAN networks, which consists of three phases: 1) pre-deployment phase:-Before the deployment of a new 6LoWPAN node, a system parameter list {p, q, a, b, P, n, h, G1, G2, e, H1, H2} is published through the following steps:
• Choose two coefficients a and b specifying an elliptic curve E/Fp defined by the equation y^2=x^3+ax+b mod p, where p is a k-bit prime number.
• Choose a base point P = (x,y) on E(Fp) that generates the subgroup whose prime order is n and cofactor is h.
• Let G1 is an addictive group and G2 is a multiplicative group of order p, and choose an efficient and computable bilinear mapping algorithm [16] e: G1*G1->G2.
• Let hash functions H1:{0,1}*->Zq and H2:{0,1}*G1 where q is a prime number.
2) authentication and key establishment phase -: in this phase ,we have The 6MN, the 6MAG, the LMA and the AAA will exchange eight messages to achieve a mutual authentication.
3) handover phase.-:: Most existing schemes require that the authentication procedure is performed when each 6MN attaches to a new 6MAG resulting in a longer handover latency and heavy workload.
3. The security analysis of the proposed scheme by using AVISPA is presented-:
A. Formal Verification-:AVISPA is a formal verification tool which can automatically validate the network security protocols and applications.
B. Ability against Malicious Attacks-:1)Replay Attack::-It is an action to send the previous obtaind message to a reciever.
2) Man-in-the-middle (MITM) Attack::-By SPAM, since a group key PSK is shared among the MAGs and the LMA, any MAG can derive the message encrypted by the PSK and reencrypt.
3) Impersonation Attack::-Launched by an adversary disguising as a legitimate party in the system.
4) Privileged Insider Attack::-: An insider attack is launched by a legal and authorized entity, who has a right to access the confidential information of its organization, to steal the security data or inject fraudulent data to the system.
5) Sybil Attack::-An attacker can forge multiple identities to cheat the 6MAGs or the LMA that many legal devices are communicating with them leading to too much network resources consumed.
4. The evaluation of performance of the proposed scheme is demonstrated.:-
In this part ,we have comparision of PBSMS and SPAM scheme performance in term of computational overhead.
In SPAM uses simple hash functions and symmetric encryption which causes less time consumption, it has some security problems that need to be solved.
In , the PBSMS employs more complicated algorithms for devices which have more capability to perform bilinear pairing.
The total computational overhead in the authentication by the PBSMS is higher than that of the SPAM.

Comparison and analysis of algorithms/techniques/systems you are comparing

S. NO.	Paper Title	Working Model	Advantages	Limitations
1	**A survey on Techniques for Securing 6LoWPAN**	Technique MT6D,survey on techniques used for securing 6LoWPAN from different attacks.	This survey help in securing 6LoWPAN from different attacks and aims to assist the researchers and application developers to provide baseline reference to further carry out their research in this field.	MT6D is the only technique which provides security solution from both Internal as well as External attacks.
2	**6LoWPAN multi-layered security protocol based on IEEE 802.15.4 security features**	A new multilayer security protocol based on the security specifications of the IEEE 802.15.4.	Multilayer Security can operate at both the MAC and the 6LoWPAN adaptation layers in order to ensure all essential security aspects to broad public and industrial acceptance	Several security attacks is the limitation for deploying Multilayer Security
3	**Design of Embedded Secure Gateway Based on 6LoWPAN**	Connects wireless sensor network with IPv6 network.	The introduction of IPv6 to sensor networks brings advantages of IP network. With the gateway, users not only directly communicate with sensor nodes, but also query historical data in the web server	IPv6 has some secutrity issues which is to be developed.
4	**Implementation of Secure 6LoWPAN Communications for Tactical Wireless Sensor Networks**	Security mechanisms to be implemented on a tactical WSN using the 6LoWPAN protocol for use by the United States Marine Corps (USMC)	The use of a structured/centralized network design allows for secure network reachability and accessibility.multiple security mechanisms within the 6LoWPAN protocol which include encryption, authentication and integrity.	A limited amount of research has been conducted implementing a proposed security framework over a multi-hop 6LoWPAN network.

5	**A PMIPv6 -based Secured Mobility Scheme for 6LoWPAN**	A hybrid cryptographic method has been used to provide secure information exchanges among the 6MNs, the 6MAGs, the LMA and the AAA server.The PBSMS scheme has been proposed to enhance the security functionality of the 6LoWPAN networks	Secure and Optimized Authentication Scheme in Proxy Mobile IPv6 (SOAS-PMIPv6) to reduce Handover Latency	MNs suffered from considerable latency and packet loss during handovers even within the PMIPv6 domain. The number of signalling messages required for handover is also high.

CONCLUSION::-

- Security is a prime concern in any network. With the addition of new layer that is 6LoWPAN; additional attack also came into picture.We have proposed survey on Security mechanism and all technique with some advantages and disadvantages.
- Hop-by-hop and end-to-end security used for security in 6LoWPAN networks. Based on the IEEE 802.15.4 security features, we proposed a Combined security protocol addressing attacks inside and outside the 6LoWPAN.
- SNEP is adopted to implement encryption and authentication of wireless communication In
- Embedded Secure Gateway Based on 6LoWPAN.
- 6LoWPAN protocol for tactical WSNs. We examine the need for 6LoWPAN in tactical WSNs used by the Marine Corps in operational scenarios.
- The PBSMS(A PMIPv6-based Secured Mobility Scheme) scheme has been proposed to enhance the security functionality of the 6LoWPAN networks. A hybrid cryptographic method has been used to provide secure information exchanges among the 6MNs, the 6MAGs, the LMA and the AAA server.

Summary of analysis and possible improvements :

- Only one technique MT6D proposed in the paper but need some improvement because of some additional attack.
- In PMIPv6 -based Secured Mobility Scheme for 6LoWPAN **,**Packet loss is mitigated by using a buffering scheme and handover latency is reduced with the help of a triggering scheme.
- In Tactical Wireless Sensor Networks,cyber security mechanisms to be implemented on a tactical WSN using the 6LoWPAN protocol for use by the United States Marine Corps (USMC).Modified 6LoWPAN enabled IEEE 802.15.4 frame structure to facilitate the newly developed keying and centralized routing mechanisms.Showd the effectiveness and efficiency of the developed cyber security mechanisms to provide integrity and reliability to a deployed tactical WSN.
- Still 6LoWPAN has security vulnerabilities which explodes many kinds of network attack. So that has to be investigated.
- 6LoWPAN is less secure than Zigbee (Zigbee Is A Worldwide Standard For Low Power Mesh Networks For Home And Buildings) and it also supports

short-range without mesh topology. Lastly, if compare to interference, it has less immunity than wifi or Bluetooth devices.

- The current challenges in maintaining the security of embedded systems are:-----
  - embedded devices are not vulnerable to cyberattacks,
  - embedded devices are not attractive targets for hacking.
  - embedded devices get sufficient security with encryption and authentication.

References-:

A survey on Techniques for Securing 6LoWPAN:-Kushalnagar, N., Montenegro, G., and C. Schumacher, "IPv6 over LowPower Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals", RFC 4919, August 2007

6LoWPAN multi-layered security protocol based on IEEE 802.15.4 security features: N. Kushalnagar, G. Montenegro, and C. Schumacher, “Ipv6 over lowpower wireless personal area networks (6lowpans): overview, assumptions, problem statement, and goals,” Tech. Rep., 200

Design of Embedded Secure Gateway Based on 6LoWPAN: G. Montenegro , N. Kushalnagar, J. Hui, D. Culler, Transmission of IPv6 Packets over IEEE 802.15.4 Networks, RFC4944, http://www.ietf.org/rfc/rfc4944.txt' September,2007

Implementation of Secure 6LoWPAN Communications for Tactical Wireless Sensor Networks:Unattended Ground Sesnor Set AN/GSQ-257 Technical Manual, TM 09632A-OI, U.S. Marine Corps, Washington, DC, 2008.

A PMIPv6 -based Secured Mobility Scheme for 6LoWPAN: D. Johnson, C. Perkins, and J. Arkko, “Mobility Support in IPv6,” IETF RFC 3775, 2004.

IOT MINOR-1
NAME-SHANU KUMAR
Roll NO.: 187159
SEC-A
CLASS: B.TECH 4TH YR CSE