Security from Denial of Sleep Attack in Wireless Sensor Network

Simerpreet Kaur, Md. Ataullah, Monika Garg
Department of Computer Science and Engineering, Phagwara, India
simerpreet3@gmail.com
Department of Computer Science and Engineering, Phagwara, India
mdataullah@ymail.com
Department of Computer Science and Engineering, Phagwara, India
monikagarg.lpu@gmail.com

ABSTRACT

With the advancement in Wireless Sensor Network (WSN) sensors are gaining importance in the physical world. Besides the low power of sensor nodes used, sensors are widely used in detecting temperature, pollution, pressure and other various applications. Energy-constrained sensor networks periodically place nodes to sleep in order to extend the network Lifetime. Denial of sleep attacks are a great threat to lifetime of sensor networks as it prevents the nodes from going into sleep mode. In this paper we are describing prevention against Denials of sleep attack. We have analyzed each of proposed solutions, identify their strengths and limitations.

Indexing terms

Wireless Sensor Network (wsn), Denial of sleep, Medium Access Control (MAC), Heterogeneous Network, Cluster.

INTRODUCTION

Wireless sensor network (WSN) consist of several nodes where each node is connected to one or more sensor. WSN have applications in many important areas, such as the military, homeland security, health care, the environment, agriculture, and manufacturing. Providing security in Sensor networks are not an easy task. Compared to conventional desktop computers, severe constraints exist since sensor nodes have limited processing capability, storage, and energy, and wireless links have limited bandwidth.

The most energy consumption attack in wsn is denial of sleep attack in which attacker consumes the sensor nodes energy by making it nodes wake even when there is no traffic to hold. In this way sensor nodes energy is consumed totally and sensor nodes die. Due to which the lifetime of the wireless sensor network decreases by causing the radio of the receiver ON draining the battery in only few days. Energy is wasted due to Collision, Overhearing, and Control packet overhead and Over-emitting. When the receiver node receives more than one packet at a time collision occurs and has to be discarded and retransmitted which increases the energy consumptions. Overhearing occurs when the node receive a packet destined for other node which causes the receiving node energy consumption by keeping its radio on. The third energy consumption problem is control packet overhead where the minimum number of control packets are send for the data transmission as the staying the node wake for control packets consume the battery life. Control packets are RTS (request to send) and CTS (clear to send).The last reason for energy consumption is caused by the transmission of the message when the destination node is not ready to receive. This energy consumption attacks are performed on Data link layer. Data link layer are divided into LLC (Link layer control) and MAC (medium access control) layer. MAC layer is used to overcoming this energy consumption attack.

From this it can be understood that security against the denial of sleep attack is a very important part.

Due to the importance of this problem, there have been several solutions, proposed to solve it. In this paper we will describe WSN and analyze each of these solutions, identify their strengths and limitations.

The rest of this paper is organized as follows. In Section II WSN is described and several possible denial of sleep attacks are outline. Section III gives the detailed of some attack scenarios. Section IV provides a description of the existing solutions to deal with Denial of sleep attacks. In Section V we provide a comparison of the characteristics and features of these solutions. In Section VI we conclude.

PROBLEM DEFINITION

Wireless Sensor Networks

Wireless sensor network (WSN) have limited processing capability and memory. Wireless sensor network consist of several nodes where each node is connected to one or more sensor. Fig 1 shows Sensor Node structure where sensor node consist of battery operated sensing unit consisting of sensor and ADC (analog to digital converter), Memory unit having one of the microcontroller or microprocessor and communication unit consisting of radio and an antenna.

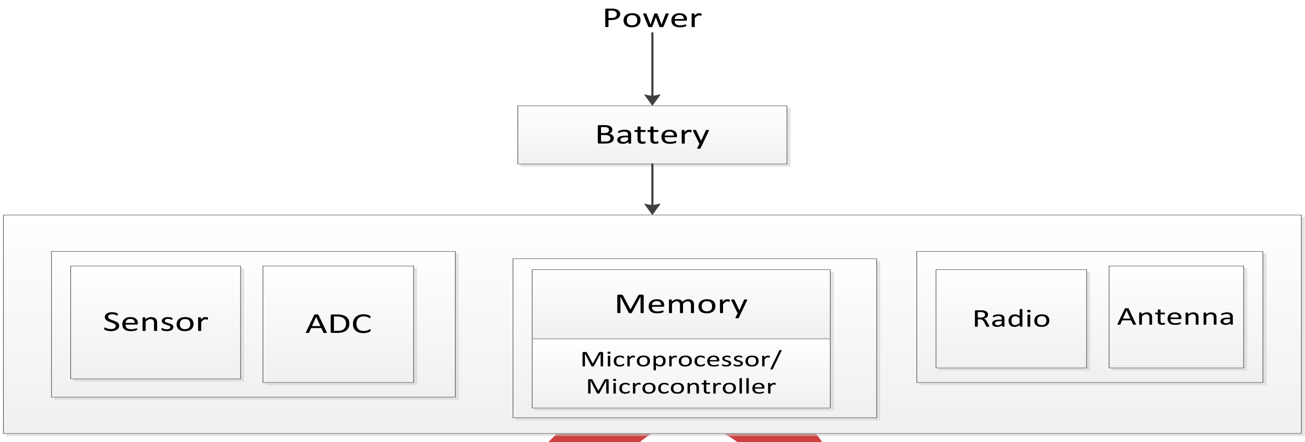


Fig 1: Sensor node Structure

Fig 2 shows Sensor Network Architecture where we have a region where sensor nodes operate, this region is known as sensing region. And the sink which send the queries or commands to the sensor nodes in the sensing region while sensor nodes collaborate to accomplish the sensing task and send the sensed data to sink .The Sink also serves as the gateway to internet as it collect and processing the data getting from sensor nodes and send the data to the user through internet. Further to send the data to sink the sensor node can use either of following architecture.

Single hop architecture- It is used for the long distance communication, due to which it takes more energy consumption communication overhead so it is costly.

Multihop architecture- Sensor nodes are densely deployed and the neighbor nodes are close to each other so the data is send through the intermediate nodes to the sink. Further Multihop architecture is divided into two types:

- Flat architecture: Here each node plays the same sensing task and there is no global identifier in a sensor network.
- Hierarchical architecture: Here sensor nodes are divided into the clusters, where cluster members send their data to cluster head and which further send the data to the sink.

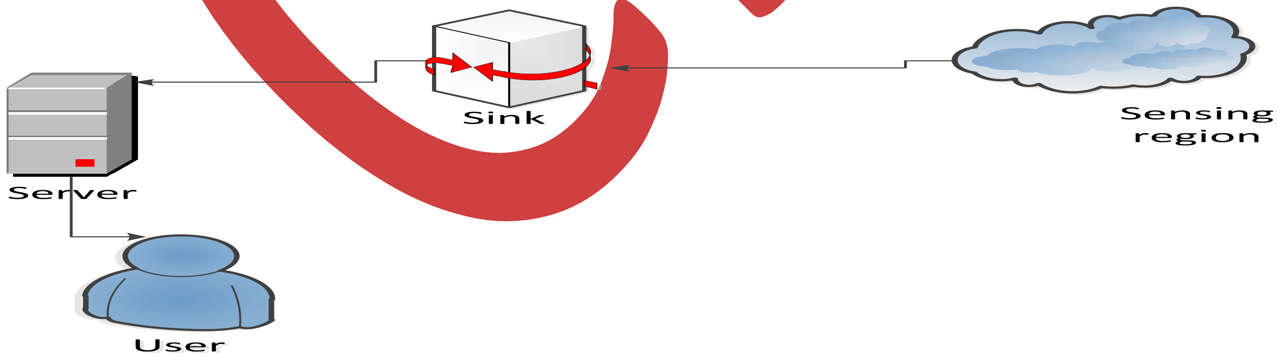


Fig 2: Sensor Network Architecture

The protocol used in sensor networks is shown in Fig 3. Here protocol stack have been divided into group of management plane across each layer. The power management plane is responsible for managing power level of sensor node for sensing and processing. The connection management plane is responsible for configuration and reconfiguration of sensor nodes to establish and maintain the connectivity of network. The task management plane is responsible for task distribution among sensor nodes in sensing region. Other protocol layers have similar operation as in wireless network protocol.

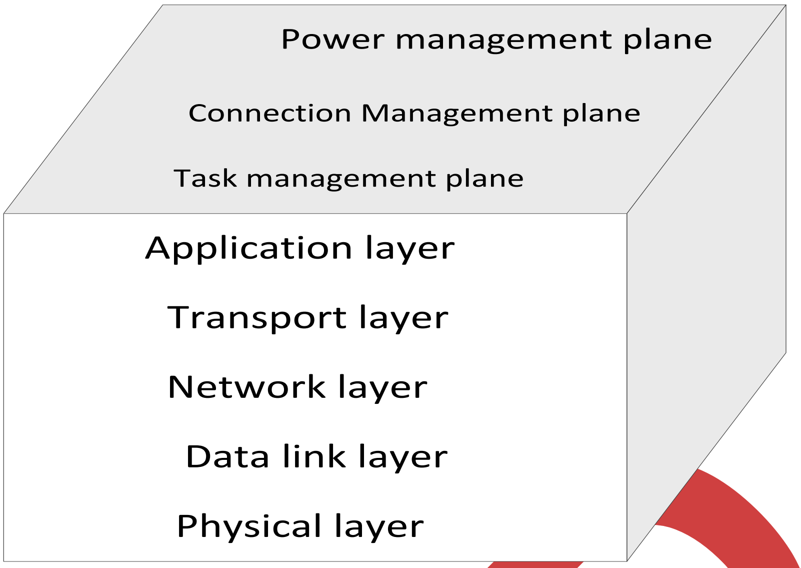


Fig 3: Protocol Stack for Wireless Sensor Network

Denial of Sleep Attack

It is a technique which prevents the radio from going into sleep mode. Many techniques introduced its impact on battery –powered mobile devices. An attacker might uses jamming attack to consume the energy and battery of the sensor but it would take about months to completely deplete the targeted devices whereas denial of sleep attack is a clever attack that keeps the sensor nodes radio ON that drain the battery in only few days. Several solutions have been proposed to solve these types of attack but each has limited feature which are only concern to the particular layer. In this paper we are only concern with the denial of sleep attack which is type of denial of service attack on data link layer.

MAC Layer

Data link layer is divided into two sub layer MAC layer and Link layer. The link layer coordinates the access to the physical medium linking a network node. The link layer decides when the radio should transmit frames; listen to the channel to receive data and sleep to conserve energy. MAC protocols operate at link layer and these protocols are used for detecting denial of sleep attacks because they control the functionality of the transceiver, which consumes more energy than any other components. The MAC protocol is responsible for managing the radio of sensor, and radio is main source of power consumption. To design a secure MAC layer it is crucial to understand the normal and malicious sources of energy loss, which is essential to design the power control system.

VARIOUS TYPES OF ATTACK

Most of the research in WSN security has concentrated on the confidentiality and integrity of the data in the network. Due to the limited energy of a WSN, it remains extremely vulnerable to security attacks draining the most critical resource. Different security attacks, which amplify the energy drains and delays, can majorly affect the performance of the MAC layer. The effect of these attacks on the MAC layer performance can be minimized or removed, if the behavior of the attacks is analyzed and modeled. It enlightens the sequence of activities perform by attacker or malicious node. The following subsections explain the main MAC security attacks in detail.

Collision Attack

The malicious collision attack can be easily launched by a compromised sensor node. In a collision attack, a malicious node does not follow the MAC protocol rules and causes collisions with neighboring nodes' transmissions by sending a short noise packet. This attack does not consume much energy of the attacker but can cause a lot of disruptions to the network operation. It is difficult to detect this attack because of the broadcast nature of the wireless environment.

Unintelligent Attack

In case of the unintelligent replay attack, the attacker does not have MAC protocol knowledge and no ability to penetrate the network. Here, recorded events are replayed into the network which prevent nodes from entering sleep mode and lead to waste in energy in receiving and processing the extra packets. If nodes are not equipped with an anti-replay mechanism this attack causes the replayed traffic to be forwarded through the network, consuming power at each node on the path to the destination. The replaying of events has adverse effect on the network lifetime and overall performance of WSN.

Unauthenticated Broadcast attack

In an unauthenticated broadcast attack, the attacker has full knowledge of the MAC protocol but does not have the capability to penetrate the network. Here, the attacker broadcasts the unauthenticated traffic into the network by following all MAC rules. These unauthenticated and unnecessary broadcasts messages are disturbing the normal sleep and listen cycle of the node and place most of the nodes in listen mode for an extended amount of time; it leads to increase in energy consumption and reduction in network lifetime. These attacks cause server harm to MAC protocols that are having short messages and short adaptive timeout period.

Full Domination attack

Here, the attacker has full knowledge of the MAC layer protocol and ability to penetrate the network. This type of attack is one of the most destructive to a WSN as the attacker has the ability to produce trusted traffic to gain the maximum possible impact from denial of sleep. The attacks are mounted using one or more compromised nodes in the network. All kinds of MAC layer protocols are vulnerable to this kind of attack.

Exhaustion attack

The attacker who commences an exhaustion attack [10] has knowledge about the MAC protocol and the ability to penetrate the network. These attacks are possible only in case of request to send (RTS)/clear to send (CTS) based MAC protocols. In this attack, the malicious node sends RTS to a node and if the node replies with CTS, the malicious node will repeatedly transmit the RTS to the node, which will prevent the node from going into sleep mode and instead drain the total energy of the node. These attacks are affecting the node lifetime and can partition the network.

Intelligent Jamming attack

The intelligent jamming attack is one of the most disastrous attacks where attacker has full protocol knowledge but does not have the ability to penetrate the network. The attacker injects unauthenticated unicast and broadcast packets into the network. These attacks can differentiate between control traffic and data traffic and unlike the unauthenticated replay attack it replays the selective events (control or data).

RELATED WORK

Recently, there have been several existing solutions to solve the Denial of sleep attacks problem by adding security to WSN in order to prevent/detect attacker. However, most of them have some critical drawbacks. They are described below in compact form with their strengths and limitations as follows:

Wireless sensor network denial of sleep attack

Brownfield et al. [4] proposed new MAC protocol which mitigates many of the effects of denial of sleep attacks by centralizing cluster management. MAC has several energy saving features which not only extend the network lifetime, but the centralized architecture makes the network lifetime more resistant to denial of sleep attacks.

Other than single period and synchronization message, it has two contention period and different networks for sending the message within the clusters and outside the cluster through the gateway node. The MAC protocol Performance Results show that G-MAC performs signifantly better than other protocols in every traffic situations. The empty network case shows the protocol overhead and idle listening effects determined by the effective duty cycle-MAC has .95% duty cycle is weighted average of duty cycle of gateway node and other nodes. Attacker can gain access to network through gateway node. But attacker can only affect one node at a time because nodes alternate the gate way responsibilities based upon incremental increase in battery levels.

Effect of Denial of sleep attacks on wireless sensor network MAC protocols

David R. Raymond et al. [5] classifies sensor network denial-of-sleep attacks in terms of an attacker's knowledge of the medium access control (MAC) layer protocol and ability to bypass authentication and encryption protocols. Attacks from each classification are then modeled to show the impacts on four sensor network MAC protocols, i.e., Sensor MAC (S-MAC), Timeout MAC (T-MAC), Berkeley MAC (B-MAC), and Gateway MAC (G-MAC).

Implementations of selected attacks on MAC, T-MAC, and B-MAC are described and analyzed in detail to validate their effectiveness and analyze their efficiency. And it shows that the most efficient attack on S-MAC can keep a cluster of nodes awake 100% of the time by an attacker that sleeps 99% of the time. Attacks on T-MAC can keep victims awake

100% of the time while the attacker sleeps 92% of the time. With knowledge of protocol because of differences exist in packet structure and timing between WSN MAC protocols, and even without ability to penetrate encryption; all wireless sensor network MAC protocols are susceptible to a full domination attack, which reduces the network lifetime to the minimum possible by maximizing the power consumption of the nodes' radio subsystem.

Even without the ability to penetrate encryption, subtle attacks can be launched, which reduce the network lifetime by orders of magnitude. If sensor networks are to meet current expectations, they must be robust in the face of network attacks to include denial-of-sleep. This approach also increases the network overhead.

Clustered Adaptive Rate Limiting: Defeating Denial-Of-Sleep Attacks In Wireless Sensor Networks

Raymond D. R. et al. [6] describes the host based lightweight intrusion detection technique, Clustered Adaptive Rate Limiting (CARL) based on rate limiting approach at MAC layer is proposed to defeat denial of sleep attacks.

The primary shortcoming of above technique is that the period during which nodes are awake is not synchronized, so if a node has packet to send, there is no guarantee that other nodes will poll at proper time to overhear a portion of preamble and remain awake for the data packet. The technique used in B-MAC increases latency in multi hop networks and if bursts of network traffic are generated at a higher rate than is supported by rate-limiting policy, network traffic is lost.

So in adaptive rate limiting, network traffic is restricted only when malicious packets have been sensed at a rate sufficient to suspect the attack. . It can be used to maintain network lifetimes and better throughput at a time even in face of sleep deprivation attack.

An Effective Scheme for Defending Denial-of-Sleep Attack in Wireless Sensor Networks.

Chen C. et al. [7] describe a scheme is proposed employing fake schedule switch with RSSI measurement aid. Here we focus on previous attack and introduce fake schedule. The sensor nodes can reduce and weaken the harm from exhaustion attack and on the contrary make the attackers lose their energy quickly so as to die. Simulation results show that at a bit price of energy and delay, network health can be guaranteed and packets drop ratio has been decreased compare with original scenario without our scheme. Here in this paper we consider only S-MAC protocol with duty cycle 10%. If packet loss is not caused by the attack, then fake schedule switch is harmful. Due to which RSSI is used as a value assigned to each node and node having attacker one hop away has larger RSSI value.

Sleep deprivation Attack Detection in Wireless Sensor network

Tapalina Bhattasali et al. [8] proposed a hierarchical framework based on distributed collaborative mechanism for detecting sleep deprivation torture in wireless sensor network efficiently.

In heterogeneous sensor field, sensor nodes are categorized into various roles such as sink gateway (SG), sector monitor(SM), Sector-in –charge (SIC) and leaf node (LN) depending on their battery capacity. Here leaf node is used to sense the data, SIC is used to collect the data and SM detect the data as valid data and invalid data. Sink Gateway is used to access other networks.

Here if leaf nodes are directly affected by intruder, node cannot detect it. As a result battery of affected node may be low or exhausted completely. This can affect data transmission for network due to which it is done in authenticated way.

Optimal Dynamic Sleep Time Control in wireless Sensor Networks

Ning et al. [9] proposed the dynamic sleep time rather than fixed sleep time which minimizes the energy wasted in idle channel i.e. energy to transmit and receive the message. This paper has used the dynamic programming (DP) algorithm rather than differential equations (ODE) to find the global optimal solution.

Problem with this approach is that there are some cases where it is not possible to find global optimal solution using DP, therefore ODE has to be used which is difficult to implement and is complex.

Distributed Wake-Up scheduling for Data collection in tree-based wireless sensor networks

Fang-Jing wu et al. [10] stated a scheme known as distributed wake-up scheduling scheme for data collection in a sensor networks that achieves both energy conservation and low reporting latency, i.e. in a multihop wireless network, a simple and efficient way of defining interference neighbors is to prohibit a node from using the same slot0code as those of its 1-hop and 2-hop neighbors. Power saving and latency are improved to prolong network lifetime and freshness of data. Here in this scenario, since not all nodes are involved in the communication and communication directions are always toward the sink, a node only need to consider a tighter set of interference neighbors and other drawback is that this scheme cannot handle the multiple tasks at a same time.

COMPARISON OF EXISTING WORK

From the description of each of the solutions presented in Section IV, we can easily notice that no solution offers a feasible solution for the Denial of sleep attacks. Out of the all proposed solutions to solve the problem of Denial of sleep attacks, the solutions based on MAC protocol[4] have caused some serious performance penalty, the single point of failure is possible. Proposed by David R. Raymond, et al. [5] is used to analysis each MAC protocol with various types of denial of sleep attacks by forming a framework but this solution increases the network overhead. The CARL technique proposed by Raymond D. R. et al. [6] fails when network traffic is generated at higher rate than is the rate –limiting policy. The fake schedule switch solution proposed by Chen C. et al. [7] is the most ambitious ones, but either they require complex installations. On the other hand, proposed by Tapaline Bhattasali et al. [8] is comparatively more effective but leaf nodes are directly attacked by the intruder. The solution proposed by Ning et al. [9] is used to find the dynamic sleep time but solution becomes complex in some cases. Other solution proposed by Fang-Jing wu, is not able to handle multiple tasks at a same time.

PROPOSED APPROACH

The problem of hierarchical framework [8] of attack on leaf node of the cluster can be overcome by using the fake switch schedule [7] at the leaf node of cluster by calculating the RSSI value of the attacker node by the sector node. Attacks on the leaf node during its active state now can be handled. One by using the detection technique at the sector node and other using fake schedule at leaf node. Detection technique is used when the malicious packet is send through the leaf node, while fake schedule switch method is used when same message in send to leaf node again and again. Using this method the lifetime of the sensor leaf node increases as node is able to go into sleep mode and the result of which the lifetime of the cluster also increases.

CONCLUSION

This paper described WSN, several possible Denials of sleep attacks, some of the types of denial of sleep attack. We analyzed several currently available solutions; identify their strengths and limitations and provide comparison among them. So we can say that this paper may be used as a reference by researchers when deciding how to secure the sensor nodes. We are also working on developing a solution of securing the sensor nodes in the clusters, so that we can make sure sensor nodes is able to cope up with attacks.

REFERENCES

[1] Wireless Sensor Network: A Networking Perspective by Jun Zheng and Abbas Jamalipour, Kenneth Moore, Director of IEEE Book and Information Services (BIS)Jeanne Audino, Project Editor.

[2] David R.Raymond and Scott F.Midkiff Virginia tech (2008): “Denial of service in wireless sensor networks; attacks and defenses”, published by IEEE CS 2008.

[3] Manju.V.C (2005): “Analysis of Denial of Sleep Attack in WSN”, International conference on Recent Development in Engineering and technology.

[4] Michael Brownfield, Yatharth Gupta, Mem and Nathaniel Davis IV (2005):” Wireless Sensor Network Denial of sleep attack” published by IEEE 2005.

[5] David R. Raymond, Randy C. Marchany, Michael I. Brownfield, and Scott F. Midkiff, (2009): “Effect of Denial of sleep attacks on wireless sensor network MAC protocols” published by IEEE 2008.

[6] Raymond D. R., Midkiff S. F (2007), “Clustered Adaptive Rate Limiting: Defeating Denial-Of-Sleep Attacks In Wireless Sensor Networks”, Military Communications Conference, 2007, MILCOM 2007, IEEE, pp. 1-7.

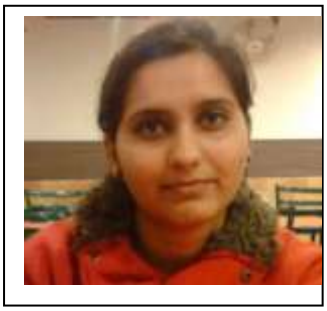
[7] Chen C., Hui L., Pei Q., Ning L., Qingquan P. (2009) , “An Effective Scheme for Defending Denial-of-Sleep Attack in Wireless Sensor Networks”, Proceedings of the 2009 Fifth International Conference on Information Assurance and Security, Vol. 02, IEEE CS, Washington DC, USA, ISBN: 978-0-7695-3744-3, DOI:10.1109/IAS.2009.33.

[8] Tapalina Bhattasali, Rituparna Chaki, Sugata sanyal (2012): “Sleep deprivation Attack Detection in Wireless Sensor network”, International Journal of Computer Applications, February 2012.

[9] Xu Ning and Christo G. Cassandras (2008): “Optimal Dynamic Sleep Time Control in Wireless Sensor Networks”, IEEE Conference on Decision and Control Cancun, Mexico, Dec. 9-11, 2008.

[10] Fang- Jing Wu and Yu-Chee Tseng (2009): “Distributed Wake-up Scheduling for Data collection in tree-based wireless sensor networks” published by IEEE Communications letters, Vol. 13, No.11, November 2009.

Author’ biography



Simerpreet Kaur received her B.tech degree in Computer Science from Himachal Pradesh University, Shimla (HP), India, in 2011 and currently pursuing her M.tech degree in Computer Science from Lovely Professional University (LPU), Phagwara, India. Her research interests include Wireless sensor networks and Artificial intelligence.

Md.Ataullah received his M.Tech degree from National Institute of Technology, Hamirpur, India. He is currently working as Assistant Professor in Lovely Professional University (LPU).His area of research is ARP, E-ARP, Wireless sensor networks and Cloud Computing.

Monika Garg received her B.Tech degree in Computer Science Ideal Institute of technology, Ghaziabad, U.P. India, in 2010 and pursuing M.Tech Degree in Computer Science from lovely University (LPU), India. Her research area include MANET, Network Security.