Volume 3, Issue 12, December 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Survey of Mobile Ad Hoc Network Attacks

Pramod Kumar Soni
M Tech Scholar CDLU SIRSA
India

Mrs, Sangeeta
Asst. Prof. CDLU SIRSA
India

Manoj Kumar Sharma
IA SPU Jodhpur
India

***Abstract*— Security is an essential requirement in mobile ad hoc network (MANETs). Compared to wired networks, MANETs are more vulnerable to security attacks due to the lack of a trusted centralized authority and limited resources. Attacks on ad hoc networks can be classified as passive and active attacks, depending on whether the normal operation of the network is disrupted or not. In this paper, we are describing the all prominent attacks described in literature in a consistent manner to provide a concise comparison on attack types.**

***Keywords*— MANET, Survey, Security attacks. Routing Protocols, AODV**

I INTRODUCTION

In a MANET, a collection of mobile hosts with wireless network interfaces form a temporary network without the aid of any fixed infrastructure or centralized administration. A MANET is referred to as an infrastructure less network because the mobile nodes in the network dynamically set up paths among themselves to transmit packets temporarily. In a MANET, nodes within each other's wireless transmission ranges can communicate directly; however, nodes outside each other's range have to rely on some other nodes to relay messages. Any routing protocol must encapsulate an essential set of security mechanism. These mechanisms are used to prevent, detect and respond to security attacks. There are five major security goals that need to be addressed in order to maintain a reliable and secure ad-hoc network environment. They are as follows: Confidentiality, Availability, Authentication, and Integrity & Non-repudiation.

II Routing in MANET

Routing in ad-hoc network involves determining a path from the source to the destination data can be communicated and the delivery of the packets to the destination nodes while nodes in the network are moving freely. Due to this node mobility, a path established by a source may not exist after a short interval of time. To cope with node mobility, nodes need to maintain routes in the network. Routing protocols for ad-hoc networks broadly fall into pro-active, reactive, hybrid and location-based categories depending upon how nodes can establish and maintain paths. Routing schemes can be classified into three categories namely, table driven (or proactive) routing protocols; On Demand (or Reactive) Routing protocols and hybrid (Location Based) routing protocols In Table-driven routing protocols each node maintains one or more tables containing routing information to every other node in the network. All nodes update these tables so as to maintain a consistent and up-to-date view of the network. When the network topology changes the nodes propagate update messages throughout the network in order to maintain consistent and up-to-date routing information about the whole network. These routing protocols differ in the method by which the topology change information is distributed across the network and the number of necessary routing-related tables for example DSDV, WRP. On Demand Routing (Reactive Protocols) these protocols take a lazy approach to routing. In contrast to table-driven routing protocols all up-to-date routes are not maintained at every node, instead the routes are created as and when required. When a source wants to send to a destination, it invokes the route discovery mechanisms to find the path to the destination. The route remains valid till the destination is reachable or until the route is no longer needed. This section discusses a few on-demand routing protocols for example DSR, AODV. Ad hoc on-demand Distance Vector Routing (AODV) Ad hoc On-demand Distance Vector Routing (AODV**)** is an improvement on the DSDV algorithm discussed in earlier section. AODV minimizes the number of broadcasts by creating routes on-demand as opposed to DSDV that maintains the list of all the routes. AODV requires each node to maintain a routing table containing one route entry for each destination that the node is communicating with. Each route entry keeps tracks of certain fields.

III Type of Security Attacks

External vs. Internal attacks

External attacks, in which the attacker aims to cause congestion, propagate fake routing information or disturb nodes from providing services. Internal attacks, in which the adversary wants to gain the normal access to the network and participate the network activities, either by some malicious impersonation to get the access to the network as a new node, or by directly compromising a current node and using it as a basis to conduct its malicious behaviors. The security attacks in MANET can be roughly classified into two major categories, namely passive attacks and active attacks are as described in the figure 1.The active attacks further divided according to the layers.

© 2013, IJARCSSE All Rights Reserved

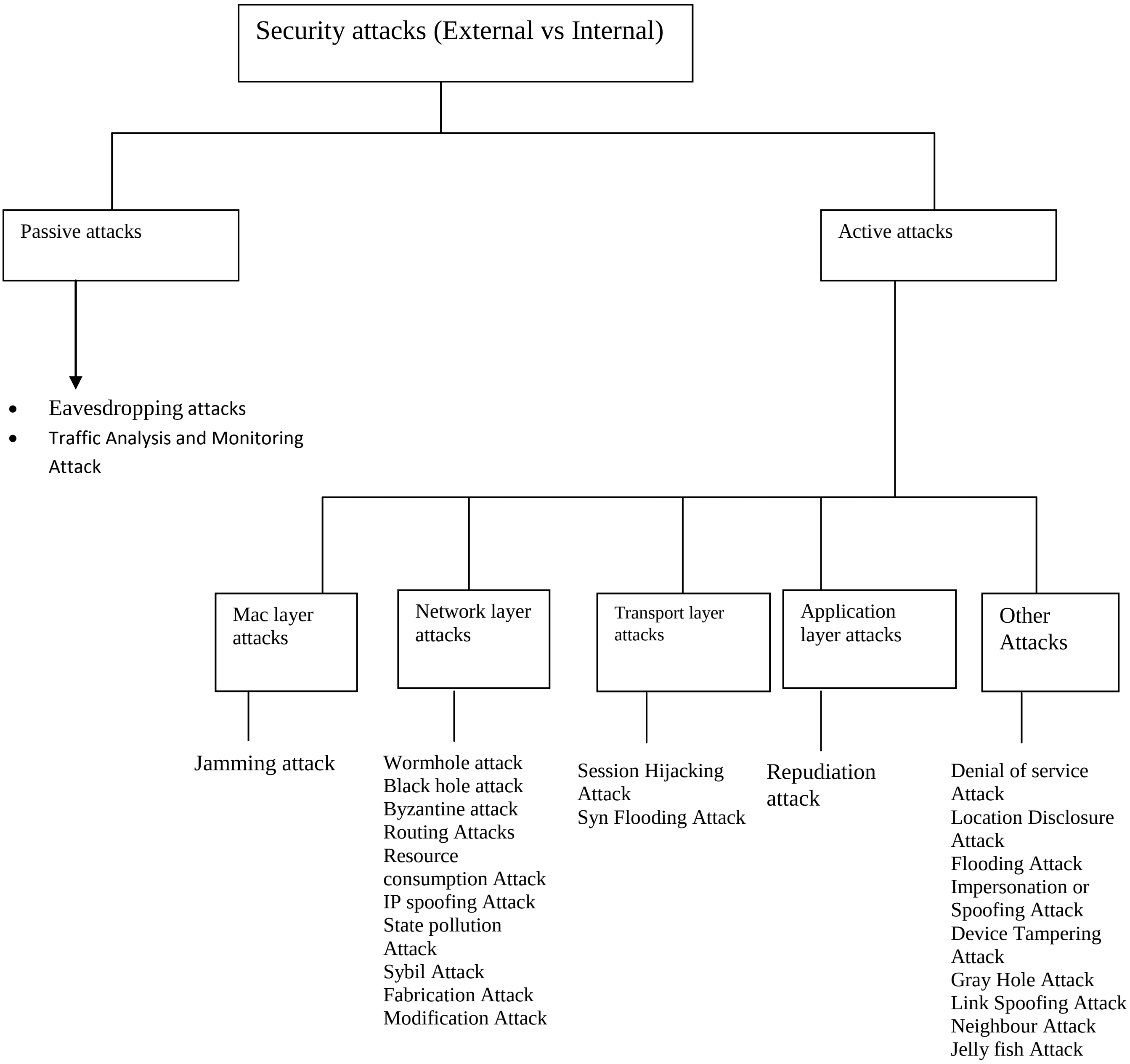

Fig. 1 types of Attacks in MANET

IV Passive **Attacks**

A passive attack does not disrupt the normal operation of the network; the attacker snoops the data exchanged in the network without altering it. Here the requirement of confidentiality gets violated. Detection of passive attack is very difficult since the operation of the network itself doesn't get affected. One of the solutions to the problem is to use powerful encryption mechanism to encrypt the data being transmitted, there by making it impossible for the attacker to get useful information from the data overhead.

Eavesdropping

Eavesdropping is another kind of attack that usually happens in the mobile ad hoc networks. It aims to obtain some confidential information that should be kept secret during the communication. The information may include the location, public key, private key or even passwords of the nodes. Because such data are very important to the security state of the nodes, they should be kept away from the unauthorized access.

Traffic Analysis & Monitoring

Traffic analysis attack adversaries monitor packet transmission to infer important information such as a source, destination, and source-destination pair.

© 2013, IJARCSSE All Rights Reserved

V. Active Attacks

An active attack attempts to alter or destroy the data being exchanged in the network there by disrupting the normal functioning of the network. Active attacks can be internal or external. External attacks are carried out by nodes that do not belong to the network. Internal attacks are from compromised nodes that are part of the network. Since the attacker is already part of the network, internal attacks are more severe and hard to detect than external attacks. Active attacks, whether carried out by an external advisory or an internal compromised node involves actions such as impersonation, modification, fabrication and replication. As shown in figure 1.

MAC LAYER ATTACKS

(i) Wormhole Attack

In the wormhole attack, an attacker tunnels messages received in one part of the network over a low latency link and replays them in a different part. The simplest instance of this attack is a single node situated between two other nodes forwarding messages between the two of them. However, wormhole attacks more commonly involve two distant malicious nodes colluding to understate their distance from each other by relaying packets along an out-of-bound channel available only to the attacker. An attacker situated close to a base station may be able to completely disrupt routing by creating a well-placed wormhole. An attacker could convince nodes who would normally be multiple hops from a base station that they are only one or two hops away via the wormhole. This can create a sinkhole: since the attacker on the other side of the wormhole can artificially provide a high-quality route to the base station, potentially all traffic in the surrounding area will be drawn through if alternate routes are significantly less attractive. This will most likely always be the case when the endpoint of the wormhole is relatively far from a base station [4].

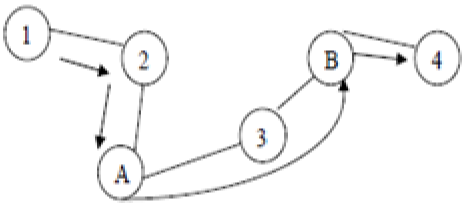

Fig.2 : Worm Hole Attack

NETWORK LAYER ATTACKS

(i) Black hole Attack

In Black Hole Attacks malicious nodes never send true control messages initially. To carry out a black hole attack, malicious node waits for neighboring nodes to send RREQ messages. When the malicious node receives an RREQ message, without checking its routing table, immediately sends a false RREP message giving a route to destination over itself, assigning a high sequence number to settle in the routing table of the victim node, before other nodes send a true one. Therefore requesting nodes assume that route discovery process is completed and ignore other RREP messages and begin to send packets over malicious node.

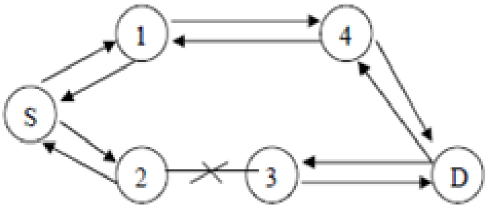

Fig 3 : Black Hole Attack

Malicious node attacks all RREQ messages this way and takes over all routes. Therefore all packets are sent to a point when they are not forwarding anywhere. This is called a black hole similar to real meaning which swallows all objects and matter. To succeed a black hole attack, malicious node should be positioned at the centre of the wireless network. If malicious node masquerades false RREP message as if it comes from another victim node instead of itself, all messages will be forwarded to the victim node. By doing this, victim node will have to process all incoming messages and is subjected to a sleep deprivation attack.

(ii) Sybil attack

In a Sybil attack a single node presents multiple identities to other nodes in the network. The Sybil attack can significantly reduce the effectiveness of fault tolerant schemes such as distributed storage and multipath. Replicas, storage partitions, or routes believed to be using disjoint nodes could in actuality be using a single adversary presenting multiple identities.[2]

© 2013, IJARCSSE All Rights Reserved

(iii) Byzantine attack

A compromised intermediate node works alone, or a set of compromised intermediate nodes works in collusion and carry out attacks such as creating routing loops, forwarding packets through non-optimal paths, or selectively dropping packets, which results in disruption or degradation of the routing services.

(iv) Routing Attacks

There are several types of attacks mounted on the routing protocol which are aimed at disrupting the operation of the network. Various attacks on the routing protocol are as follows: Routing Table Overflow, Routing Table Poisoning, Packet Replication, Route Cache Poisoning and Rushing Attack

(v) Resource consumption attack

This is also known as the sleep deprivation attack. An attacker or a compromised node can attempt to consume battery life by requesting excessive route discovery, or by forwarding unnecessary packets to the victim node.

(iv) IP Spoofing attack

In conflict-detection allocation, the new node chooses a random address (say y) and broadcast a conflict detection packet throughout the MANET. Any veto from a node will prevent it from using this address. If the malicious node always impersonates a member that has occupied the same IP address and keeps replying with vetoes, it is called an IP Spoofing attack as illustrated in below figure 04.

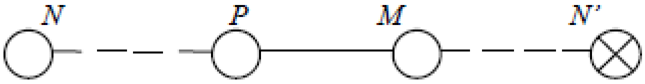

Fig 4 : IP Spoofing Attack

In figure 4, N represents the new node, and M represents a malicious node. Node P is a neighbour of node M. Although node P may be aware that it has no direct neighbour with the address of y by means of a neighbour detection mechanism, it still thinks that the veto message is forwarded by node M from another node N'.

(vii) State Pollution attack

If a malicious node gives incorrect parameters in reply, it is called the state pollution attack. For example, in best effort allocation, a malicious allocator can always give the new node an occupied address, which leads to repeated broadcast of Duplication Address Detection messages throughout the MANET and the rejection of new node.

(viii) Fabrication

Instead of modifying or interrupting the existing routing packets in the networks, malicious nodes also could fabricate their own packets to cause chaos in the network operations. They could launch the message fabrication attacks by injecting huge packets into the networks such as in the sleep deprivation attacks. However, message fabrication attacks are not only launch by the malicious nodes. Such attacks also might come from the internal misbehaving nodes such as in the route salvaging attacks.

(ix) Modification

In a message modification attack, adversaries make some changes to the routing messages, and thus endanger the integrity of the packets in the networks. Since nodes in the ad hoc networks are free to move and self-organize, relationships among nodes at some times might include the malicious nodes. These malicious nodes might exploit the sporadic relationships in the network to participate in the packet forwarding process, and later launch the message modification attacks. Examples of attacks that can be classified under the message modification attacks are packet misrouting and impersonation attacks.

TRANSPORT LAYER ATTACKS

(i) Session hijacking attack

Session hijacking takes advantage of the fact that most communications are protected (by providing credentials) at session setup, but not thereafter. In the TCP session hijacking attack, the attacker spoofs the victim's IP address, determines the correct sequence number that is expected by the target, and then performs a DoS attack on the victim. Thus the attacker impersonates the victim node and continues the session with the target.

(ii) SYN flooding attack

The SYN flooding attack is a denial-of-service attack. The attacker creates a large number of half-opened TCP connections with a victim node, but never completes the handshake to fully open the connection.

APPLICATION LAYER ATTACKS

(i) Repudiation attack

In the network layer, firewalls can be installed to keep packets in or keep packets out. In the transport layer, entire connections can be encrypted, end-to-end. But these solutions do not solve the authentication or non-repudiation problems in general. Repudiation refers to a denial of participation in all or part of the communications. For example, a selfish person could deny conducting an operation on a credit card purchase, or deny any on-line bank transaction, which is the prototypical repudiation attack on a commercial system

OTHER ATTACKS

(i) Denial of Service attack

Denial of service (DoS) is another type of attack, where the attacker injects a large amount of junk packets into the network. These packets overspend a significant portion of network resources, and introduce wireless channel contention and network contention in the MANET. A routing table overflow attack and sleep deprivation attack are two other types of the DoS attacks. In the routing table overflow attack, an attacker attempts to create routes to nonexistent nodes. Meanwhile the sleep deprivation attack aims to consume the batteries of a victim node. For example, consider the following Fig. 3. Assume a shortest path exists from **S** to **X** and **C** and **X** cannot hear each other, that nodes **B** and **C** cannot hear each other, and that **M** is a malicious node attempting a denial of service attack. Suppose **S** wishes to communicate with **X** and that **S** has an unexpired route to **X** in its route cache. **S** transmits a data packet toward **X** with the source route **S** --> **A** --> **B** --> **M** --> **C** --> **D** --> **X** contained in the packet's header. When **M** receives the packet, it can alter the source route in the packet's header, such as deleting **D** from the source route. Consequently, when **C** receives the altered packet, it attempts to forward the packet to **X**. Since **X** cannot hear **C**, the transmission is unsuccessful.

S ↔A↔ B↔ M ↔C↔ D↔ X

Fig 5: Denial of Service attack

(ii) Location disclosure attack

An attacker reveals information regarding the location of nodes or the structure of the network. It gathers the node location information, such as a route map, and then plans further attack scenarios. Traffic analysis, one of the subtlest security attacks against MANET, is unsolved. Adversaries try to figure out the identities of communication parties and analyze traffic to learn the network traffic pattern and track changes in the traffic pattern. The leakage of such information is devastating in security sensitive scenarios.

(iii) Flooding attack

In flooding attack, attacker exhausts the network resources, such as bandwidth and to consume a node's resources, such as computational and battery power or to disrupt the routing operation to cause severe degradation in network performance. For example, in AODV protocol, a malicious node can send a large number of RREQs in a short period to a destination node that does not exist in the network. Because no one will reply to the RREQs, these RREQs will flood the whole network. As a result, all of the node battery power, as well as network bandwidth will be consumed and could lead to denial-of-service.

(iv) Impersonation or Spoofing attack

Spoofing is a special case of integrity attacks whereby a compromised node impersonates a legitimate one due to the lack of authentication in the current ad hoc routing protocols. The main result of the spoofing attack is the misrepresentation of the network topology that may cause network loops or partitioning. Lack of integrity and authentication in routing protocols creates fabrication attacks that result in erroneous and bogus routing messages.

(v) Colluding misrelay attack

In colluding misrelay attack, multiple attackers work in collusion to modify or drop routing packets to disrupt routing operation in a MANET. This attack is difficult to detect by using the conventional methods such as watchdog and pathrater. Figure 4 shows an example of this attack. Consider the case where node A1 forwards routing packets for node T. In the figure, the first attacker A1 forwards routing packets as usual to avoid being detected by node T. However, the second attacker A2 drops or modifies these routing packets.

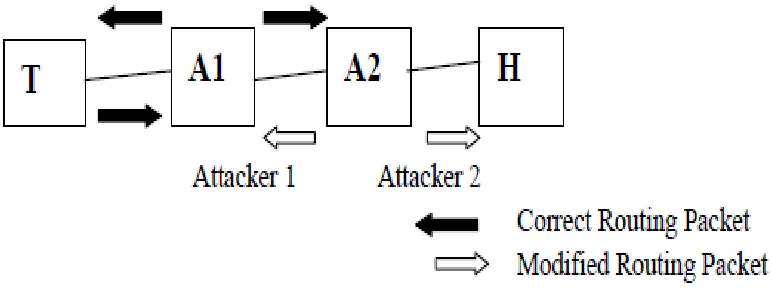

Fig 6:- Colluding Misrelay Attack

(vi) Device tampering attack

Unlike nodes in a wired network, nodes in ad hoc wireless networks are usually compact, soft, and hand-held in nature. They could get damaged or stolen easily. In the process of route discovery, control messages created by a node must be signed and validated by a receiving node. Thus the route discovery prevents anti-authenticating attacks, such as creating routing loop, fabrication because no node can create and sign a packet in the name of a spoofed or invented node. In the absence of centralized administration it is easy for MN's to change their identities.

(vii) Gray hole attack

We now describe the gray hole attack on MANETS. The gray hole attack has two phases. In the first phase, a malicious node exploits the AODV protocol to advertise itself as having a valid route to a destination node, with the intention of intercepting packets, even though the route is spurious. In the second phase, the node drops the intercepted packets with a certain probability. This attack is more difficult to detect than the black hole attack where the malicious node drops the received data packets with certainly. A gray hole may exhibit its malicious behaviour in different ways. It may drop packets coming from (or destined to) certain specific node(s) in the network while forwarding all the packets for other nodes. Another type of gray hole node may behave maliciously for some time duration by dropping packets but may switch to normal behaviour later. A gray hole may also exhibit a behaviour which is a combination of the above two, thereby making its detection even more difficult.

(viii) Link spoofing attack

In a link spoofing attack, a malicious node advertises fake links with non-neighbours to disrupt routing operations. For example, in the OLSR protocol, an attacker can advertise a fake link with a target's two-hop neighbours. This causes the target node to select the malicious node to be its MPR. As an MPR node, a malicious node can then manipulate data or routing traffic, for example, modifying or dropping the routing traffic or performing other types of DoS attacks

(ix) Neighbour attack

Upon receiving a packet, an intermediate node records its ID in the packet before forwarding the packet to the next node. However, if an attacker simply forwards the packet without recording its ID in the packet, it makes two nodes that are not within the communication range of each other believe that they are neighbours (i. e. one-hop away from each other), resulting in a disrupted route.

(x) Jellyfish attack

Similar to the black hole attack, a jellyfish attacker first needs to intrude into the forwarding group and then it delay data packets unnecessarily for some amount of time before forwarding them. This result in significantly high end-to end delay and delay jitter, and thus degrades the performance of real time applications.

VI CONCLUSION

We have discussed security issues related to integrated mobile ad hoc network (MANET)-Internet and stand alone MANET. The proposed mechanisms until now have solved many security issues related to integrated MANET-Internet communication but they have not solved them completely. So, we can design a security mechanism by which we can minimize or completely remove many of those attacks.

REFERENCES

[1] W. Stallings, *Wireless Communication and Networks*, Pearson Education,2002.

[2] C. Perkins, *Ad Hoc Networks*, Addison-Wesley, 2001.

[3] Y. Hu, D. Johnson, and A. Perrig, SEAD: Secure Efficient Distance Vector Routing in Mobile wireless Ad-Hoc Networks. *Proc. of the 4th IEEE workshopon Mobile Computing Systems and applications* (WMCSA'02).

[4] A. Tanenbaum, *Computer Networks*, PH PTR, 2003.

[5] Abhay Kumar Rai, Rajiv Ranjan Tewari & Saurabh Kant Upadhyay, "Different Types of Attacks on Integrated MANET-Internet Communication," International Journal of Computer Science and Security (IJCSS) Volume: 4 Issue: 3.

[6] Sukla Banerjee , "Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks", Proceedings of the World Congress on Engineering and Computer Science 2008 WCECS 2008, October 22 - 24, 2008, San Francisco, USA.

[7] Ping Yi, Yoe and Futai Zoo and Ning Liu, " A survey on Security in Wireless Mesh Networks", Proceedings of IETE Technical Review, Vol.27 Jan-Feb 2010

[8] Lidong Zhou J. Haas, "Securing Ad-hoc Networks", IEEE Network Magzine, 13,6, pages 24-30, 1999.

© 2013, IJARCSSE All Rights Reserved