Implementing Security Consideration in Dynamic Source Routing

Swati Dhull, Deepender Dhull, Swati Juneja

Abstract*— Security has become one of the major issues for data communication over wired and wireless networks. To enhance the security of data transmission, existing system works on the cryptography based algorithms such as SSL, IPSec. Although IPSec and SSL accounts for great level of security, they introduce overheads. A mass of control messages exchanging also needed in order to adopt multiple path deliveries from source to destination. Different from the past work on the designs of cryptography algorithms and system infrastructures, we will propose a dynamic routing algorithm that could randomize delivery paths for data transmission. The algorithm is easy to implement and compatible with popular routing protocols, such as the Routing Information Protocol in wired networks and Destination-Sequenced Distance Vector protocol in wireless networks, without introducing extra control messages. An analytic study on the proposed algorithm is presented, and a series of simulation experiments are conducted to verify the analytic results and to show the capability of the proposed algorithm.

Index Terms*— *DSR, IP, MANET, SSL, WLAN.

I. INTRODUCTION

In the past decades, various security-enhanced measures have been proposed to improve the security of data transmission over public networks. Existing work on security-enhanced data transmission includes the designs of cryptography algorithms and system infrastructures and security-enhanced routing methods. Their common objectives are often to defeat various threats over the Internet, including eavesdropping, spoofing, session hijacking, etc. Among many well-known designs for cryptography based systems, the IP Security (IPSec) and the Secure Socket Layer (SSL) are popularly supported and implemented in many systems and platforms. Although IPSec and SSL do greatly improve the security level for data transmission, they unavoidably introduce substantial overheads, especially on gateway/host performance and effective network bandwidth. For example, the data transmission overhead is 5 cycles/byte over an Intel Pentium II with the Linux IP stack alone, and the overhead increases to 58 cycles/byte when Advanced Encryption Standard (AES) is adopted for encryption/decryption for IPSec .Another alternative for security-enhanced data transmission is to dynamically route packets between each source and its destination so that the chance for system break-in, due to successful interception of consecutive packets for a session, is slim.

Manuscript received on May, 2013.

Swati Dhull, Electronics & Communication Engineering, BMIET, Sonipat, India.

Deepender Dhull, Computer Science & Engineering, IITM, Sonipat, India.

Swati Juneja, Electronics & Communication Engineering, BMIET, Sonipat, India.

The intention of security-enhanced routing is different from the adopting of multiple paths between a source and a destination to increase the throughput of data transmission. In particular, **Lou et al.** proposed a secure routing protocol to improve the security of end-to-end data transmission based on multiple path deliveries.

The set of multiple paths between each source and its destination is determined in an online fashion, and extra control message exchanging is needed. **Bohacek et al**. proposed a secure stochastic routing mechanism to improve routing security. Similar to the work proposed by **Lou et al**. a set of paths is discovered for each source and its destination in an online fashion based on message flooding. Thus, a mass of control messages is needed.

Yang and Papavassiliou explored the trading of the security level and the traffic dispersion. They proposed a traffic dispersion scheme to reduce the probability of eavesdropped information along the used paths provided that the set of data delivery paths is discovered in advance. Although excellent research results have been proposed for security-enhanced dynamic routing, many of them rely on the discovery of multiple paths either in an online or offline fashion. For those online path searching approaches, the discovery of multiple paths involves a significant number of control signals over the Internet. On the other hand, the discovery of paths in an offline fashion might not be suitable to networks with a dynamic changing configuration. Therefore, we will propose a dynamic routing algorithm to provide security enhanced data delivery without introducing any extra control messages.

II. MOTIVATION

In Static Routing, the routes are entered manually. It is the best solution when we have small networks, and the networks do not change very often. When we say change we mean new host and networks are not frequently added are removed. While dynamic route are best suited when the network structure is very dynamic. Dynamic routes use network resources to learn where all host are, and the structure of the network. To enhance the dynamic routing with security considerations, We choose randomization of path deliveries with the help of the Dynamic Routing Protocol namely DSR (Dynamic Source Routing).

III. WIRELESS NETWORK

Wireless network refers to any type of computer network that is wireless, and is commonly associated with a telecommunications network whose interconnection between nodes is implemented without the use of wires. Wireless telecommunications networks are generally implemented with some type of remote information transmission system that uses electromagnetic waves, such as radio waves, for the carrier and this implementation usually takes place at the physical level or "layer" of the network.

3.1 THREATS IN WIRELESS NETWORK

Aside from the threat of unauthorized users accessing your network and eavesdropping your internal network communications by connecting with your wireless LAN (WLAN), there are a variety of threats posed by insecure or improperly secured WLAN's. Here is a brief list with descriptions of some of the primary threats:

Rogue WLAN's – Whether your enterprise has an officially sanctioned wireless network or not, wireless routers are relatively inexpensive, and ambitious users may plug unauthorized equipment into the network. These rogue wireless networks may be insecure or improperly secured and pose a risk to the network at large.

Spoofing Internal Communications – An attack from outside of the network can usually be identified as such. If an attacker can connect with your WLAN, they can spoof communications that appear to come from internal domains. Users are much more likely to trust and act on spoofed internal communications.

Theft of Network Resources – Even if an intruder does not attack your computers or compromise your data, they may connect to your WLAN and hijack your network bandwidth to surf the Web. They can leverage the higher bandwidth found on most enterprise networks to download music and video clips, using your precious network resources and impacting network performance for your legitimate users.

Network Eavesdropping or network sniffing is a network layer attack consisting of capturing packets from the network transmitted by others' computers and reading the data content in search of sensitive information like passwords, session tokens, or any kind of confidential information. The attack could be done using tools called network sniffers. These tools collect packets on the network and, depending on the quality of the tool, analyze the collected data like protocol decoders or stream reassembling.

IV. DYNAMIC ROUTING PROTOCOL

Conceptually, the dynamic routing method has two parts: the routing protocol that is used between neighboring routers to convey information about their network environment, and the routing algorithm that determines paths through that network. The protocol defines the method used to share the information externally, whereas the algorithm is the method used to process the information internally. The routing tables on dynamic routers are updated automatically based on the exchange of routing information with other routers. The most common dynamic routing protocols are:

- Distance vector routing protocols
- Link state routing protocols

Understanding how these protocols work enables you to choose the type of dynamic routing that best suits your network needs.

4.1 DYNAMIC SOURCE ROUTING PROTOCOL

DSR is a reactive routing protocol which is able to manage a network without using periodic table-update messages like table-driven routing protocols do.DSR was specifically designed for use in multi-hop wireless networks. This protocol allows the network to be completely self-organizing and self-configuring which means that there is no need for an existing network infrastructure. For restricting the bandwidth, the process to find a path is only executed when a path is required by a node. In DSR the sender (source, initiator) determines the whole path from the source to the destination node and deposits the addresses of the intermediate nodes of the route in the packets. DSR is based on the Link-State-Algorithms which mean that each node is capable to save the best way to a destination. Also if a change appears in the network topology, then the whole network will get this information by flooding.

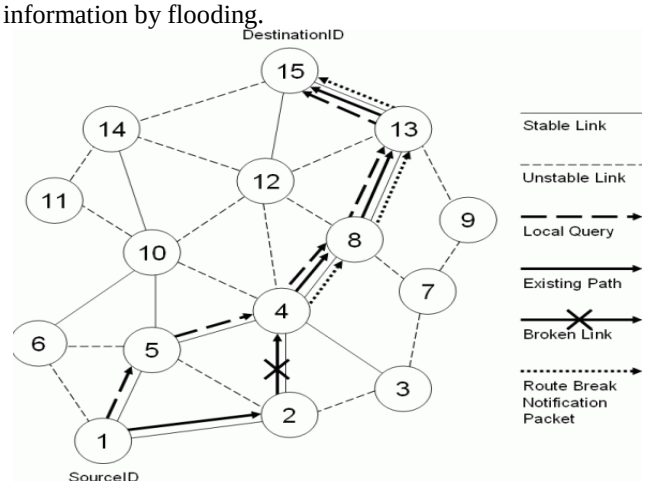

Fig1.Dynamic Source Routing

DSR contains 2 phases:

- Route Discovery (find a path)
- Route Maintenance (maintain a path)

1) ADVANTAGES: Reactive routing protocols have no need to periodically flood the network for updating the routing tables like table-driven routing protocols. Intermediate nodes are able to utilize the Route Cache information efficiently to reduce the control overhead. The initiator only tries to find a route (path) if actually no route is known (in cache).

2) DISADVANTAGES: The Route Maintenance protocol does not locally repair a broken link. The broken link is only communicated to the initiator. The DSR protocol is only efficient in networks with less than 200 nodes. Problems appear by fast moving of more hosts, so that the nodes can only move around in this case with a moderate speed. Flooding the network can cause collusions between the packets. Also there is always a small time delay at the begin of a new connection because the initiator must first find the route to the target.

V.SECURITY ENHANCED DATA TRANSMISSION

We recognize the concerns that some people have about sending personal information over the Internet and operate enhanced security measures. The transfer of personal information are completed using secure servers. These servers use high level 128 bit SSL (Secure Socket Layer) encryption - which is a leading security standard in the e-commerce industry. Some of the techniques that have been used in the existing work to enhance security were SSL and IPSec. Another alternative for security enhanced data transmission is to route the packets dynamically between each source and its destination so that the chance for system break-in, due to successful interception of consecutive packets for a session, is slim. The intention of security-enhanced routing is different from the adopting of multiple paths between a source and a destination to increase the throughput of data transmission.

5.1 SECURE SOCKET LAYER

The Secure Sockets Layer (SSL) is a commonly-used protocol for managing the security of a message transmission on the Internet. SSL has recently been succeeded by Transport Layer Security (TLS), which is based on SSL. SSL uses a program layer located between the Internet's Hypertext Transfer Protocol (HTTP) and Transport Control Protocol (TCP) layers. SSL gained the support of Microsoft and other Internet client/server developers as well and became the de facto standard until evolving into Transport Layer Security. The "sockets" part of the term refers to the sockets method of passing data back and forth between a client and a server program in a network or between program layers in the same computer. SSL uses the public-and-private key encryption system from RSA, which also includes the use of a digital certificate.

5.2 IP SECURITY

Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a data stream. IPsec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. IPsec can be used to protect data flows between a pair of hosts (e.g. computer users or servers), between a pair of security gateways (e.g. routers or firewalls), or between a security gateway and a host. IPsec is a dual mode, end-to-end, security scheme operating at the Internet Layer of the Internet Protocol Suite or OSI model Layer 3. Some other Internet security systems in widespread use, such as Secure Sockets Layer (SSL), Transport Layer Security (TLS) and Secure Shell (SSH), operate in the upper layers of these models. Hence, IPsec can be used for protecting any application traffic across the Internet. Applications need not be specifically designed to use IPsec. The use of TLS/SSL, on the other hand, must typically be incorporated into the design of applications.

VI. PROPOSED SYSTEM

To propose a dynamic routing algorithm to improve the security of data transmission. We define the eavesdropping avoidance problem as Follows: Given a graph for a network under discussion, a source node, and a destination node, the problem is to minimize the path similarity without introducing any extra control messages, and thus to reduce the probability of eavesdropping consecutive packets over a specific link. The objective of this work is to explore a security-enhanced dynamic routing algorithm based on distributed routing information widely supported in existing wired and wireless networks. We aim at the randomization of delivery paths for data transmission to provide considerably small path similarity (i.e., the number of common links between two delivery paths) of two consecutive transmitted paths. The proposed algorithm should be easy to implement and compatible with popular routing protocols, such as the Routing Information Protocol (RIP) for wired networks and Dynamic Source Routing (DSR) protocol for wireless networks**,** over existing infrastructures. This protocol shall not increase the number of control messages if the proposed algorithm is adopted. An analytic study will be presented for the proposed routing algorithm, and a series of simulation study will be conducted to verify the analytic results and to show the capability of the proposed algorithm.

6.1 ILLUSTRATION

Consider a graph for a network with source and destination node. In Distance Vector Based Routing, the routing table consists of parameters such as destination node, cost and next hop. To provide a security enhanced dynamic routing for the proposed algorithm, the routing table consist an additional parameter: history of packet deliveries to the destination node.

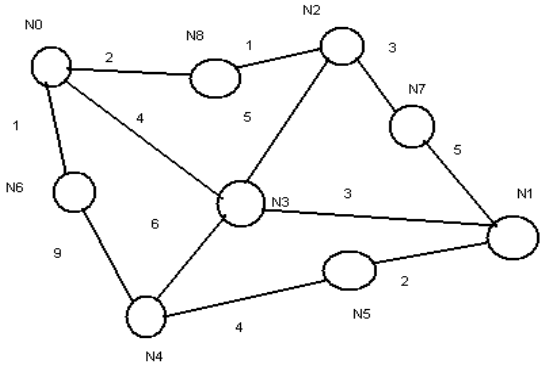

Fig2. Sample Network Topology

ROUTING TABLE COMPARISIONS

DESTINATION NODE	COST	NEXT HOP CANDIDATE
N1	**7**	N3
N2	3	N8
.....	……..	…….

Table1.routing table for original distance Vector based routing algorithm

Destination Node	Cost	Next Hop Candidate	History of Packet delivered to destination node
N1	7	{N3,N7, N5}	{(N0,N3),(N2,N7),…(N4, N5)}
N2	3	{N8,N3}	{(N0, N8),(N0,N3),… }
……	……	…….	……..

Table2.Routing table for the proposed Security enhanced routing algorithm

From the history of packet deliveries to the destination node, it will choose the next smallest path to route the packets. So that it may not be possible for the intruders to break-in.

6.2 RANDOMIZATION PROCESS

The delivery of a packet with the destination at a node. In order to minimize the probability that packets are eavesdropped over a specific link, a randomization process for packet deliveries, in this process, the previous next-hop for the source node s is identified in the first step of the process. Then, the process randomly picks up a neighboring node as the next hop for the current packet transmission. The exclusion for the next hop selection avoids transmitting two consecutive packets in the same link, and the randomized pickup prevents attackers from easily predicting routing paths for the coming transmitted packets.

ALGORITHM: RANDOMIZEDSELECTOR (s, t, pkt)

1: Let h_s be the used next hop for the previous packet Delivery for the source node s.
2: if $h_s \varepsilon C_t^{Ni}$ then
3: if $|C_t^{Ni}| > 1$ then
4: Randomly choose a node x from $\{C_t^{Ni} - h_s\}$ as a next hop, and send the packet pkt to the node x.
5: $h_s \leftarrow x$, and update the routing table of N_i.
6: else
7: Send the packet pkt to h_s.
8: end if
9: else
10: Randomly choose a node y from C_t^{Ni} as a next hop, and send the packet pkt to the node y.
11: $h_s \leftarrow y$, and update the routing table of N_i.
12: end if

DESCRIPTION

Aim: To reduce the probability of eavesdropping consecutive packets over a specific link.
Input: A Graph G with set of Nodes.
Parameters: Source Node, Destination Node and Packets.
Steps:
1. The previous next hop for the source node is identified.
2. Randomly pick up a neighboring node as the next hop for the current packet transmission.
3. The exclusion of previous hop for the next hop selection avoids transmitting two consecutive packets in the same link.
4. Randomized pickup prevents attackers from easily predicting routing paths for the coming transmitted packets.
5. Maintain the history record for each node in a hash table.
6. Before the current packet is sent to its destination node, we must randomly pick up a neighboring node excluding the used node for the previous packet.

6.3 ROUTING TABLE MAINTENANCE

In the network be given a routing table and a link table. We assume that the link table of each node is constructed by an existing link discovery protocol, such as the Hello protocol in. On the other hand, the construction and maintenance of routing tables are revised based on the well-known Bellman-Ford algorithm.

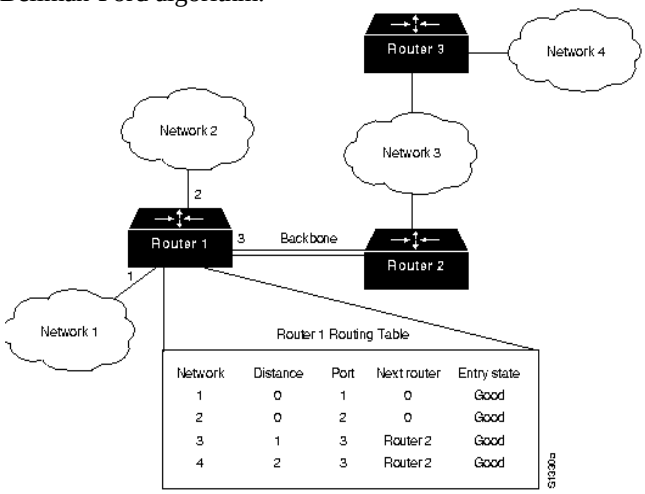

Fig3. Route Table Maintenance

VII. SIMULATION

Fig4.(a) Network Topology

Initial Network Topology with 11 nodes. Source Node is 0 and Destination Node is 10. Initially Hello Packets will be dropped by the nodes in order to establish the communication with the other nodes. The nodes retaining their full energy are indicated in Green color.

PACKET DELIVERY

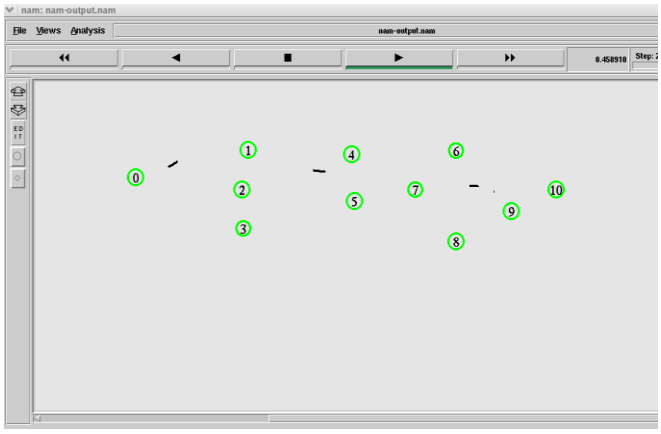

Fig4. (b) Packet Delivery

In order to forward the Packets from source to destination, an initial path is taken from the Node 0 to Node 10 through Node 1, Node 7 and Node 9. This is the first path chosen. The Packets follow this route until the node loses its energy or if the link got failure.

ENERGY LOSS

Fig 5. (c) Energy Loss

While forwarding the packets, the nodes 1 and 7 lost their energy. These nodes are indicated by Red color. These nodes

cannot send further packets. Node with survival of minimum energy is indicated by Yellow color.

CHOOSING AN ALTERNATE PATH

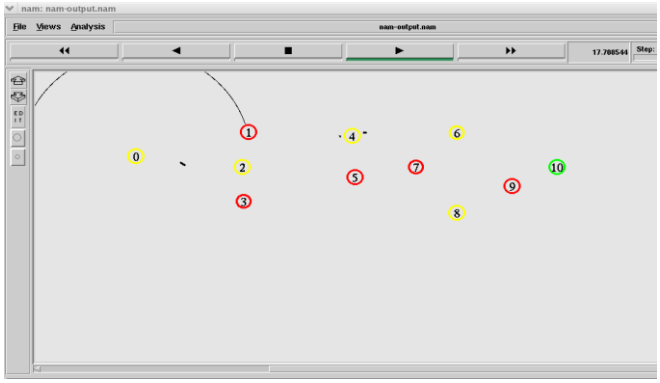

Fig 5. (d) Choosing an Alternate Path

In the above Figure, there is an indication of the failure of the first route. So, an alternate path is chosen from Node 0 to Node 10 through Nodes 2, 4,6.Similarly, they also loses their energy as they forward their packets.

FINAL TOPOLOGY

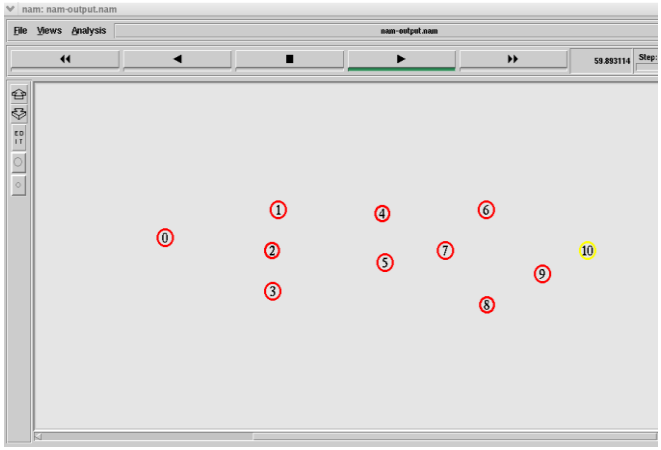

Fig 5. (e) Final Topology

Finally the Packets were forwarded and the energy has been lost for all the Nodes. Since the destination node receives the packet it also loses its energy.

VIII. CONCLUSION

We have proposed a security-enhanced dynamic routing algorithm based on distributed routing information widely supported in existing networks. The proposed algorithm is easy to implement and compatible with popular routing protocols, such as RIP and DSR, over existing infrastructures. An analytic study was developed for the proposed algorithm and was verified against the experimental results. A series of simulation experiments were conducted to show the capability of the proposed algorithm, for which we have very encouraging results. We must point out that the proposed algorithm is completely orthogonal to the work based on the designs of cryptography algorithms and system infrastructures. Our security enhanced dynamic routing could be used with cryptography-based system designs to further improve the security of data transmission over networks.

5.3 FUTURE ENHANCEMENT

Our security enhanced dynamic routing could be used with cryptography- based system designs to further improve the security of data transmission over networks. In addition to the routing information, route table maintenance is done. The energy survival of the nodes is taken into consideration. With this, the energy loses for every node as it sends or receives any packet. Once the energy loses for all the nodes in a particular path, it will take an alternate path. In that case, there will be less chance for the intruders to break-in.

REFERENCES

1) G. Apostolopoulos, V. Peris, P. Pradhan, and D. Saha, "Securing Electronic Commerce: Reducing the SSL Overhead," IEEE Network, 2000.
2) S. Bohacek, J.P. Hespanha, K. Obraczka, J. Lee, and C. Lim, "Enhancing Security via Stochastic Routing," Proc. 11th Int'l Conf. Computer Comm. and Networks (ICCCN), 2002.
3) I. Gojmerac, T. Ziegler, F. Ricciato, and P. Reichl, "Adaptive Multipath Routing for Dynamic Traffic Engineering," Proc. IEEE Global Telecommunications Conf. (GLOBECOM), 2003.
4) C. Hopps, "Analysis of an Equal-Cost Multi-Path Algorithm", Request for comments (RFC 2992), Nov. 2000.
5) S.-H. Liu, Y.-F. Lu, C.-F. Kuo, A.-C. Pang, and T.-W. Kuo, "The Performance Evaluation of a Dynamic Configuration Method over IPSEC," Proc. 24th IEEE Real-Time Systems Symp.: Works in Progress Session (RTSS WIP), 2003.
6) W. Lou and Y. Fang, "A Multipath Routing Approach for Secure Data Delivery," Proc. IEEE Military Comm. Conf. (MilCom), 2001. 38
7) W. Lou, W. Liu, and Y. Fang, "SPREAD: Improving Network Security by Multipath Routing," Proc. IEEE Military Comm. Conf. (MilCom), 2003.
8) C. Perkins and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," Proc. ACM SIGCOMM '94, pp. 234-244, 1994.
9) J. Yang and S. Papavassiliou, "Improving Network Security by Multipath Traffic Dispersion," Proc. IEEE Military Comm. Conf. (MilCom), 2001.
10) C. Kaufman, R. Perlman, and M. Speciner, "Network Security"—PRIVATE Communication in a PUBLIC World, second ed. Prentice Hall PTR, 2002.
11) Shou-heng Liu , Yung-feng Lu , Chin-fu Kuo , Ai-chun Pang , Tei-wei Kuo, "The Performance Evaluation of a Dynamic Configuration Method over IPSEC".
12) M. Faloutsos, P. Faloutsos, and C. Faloutsos, "On Power-Law Relationships of the Internet Topology," *Proc. ACM SIGCOMM '99*, pp. 251-262, 1999.
13) ER. Yashpaul Singh, and A. Swarup, "Analysis of Equal cost Adaptive Routing Algorithms using Connection-Oriented and connectionless protocol.
14) Andrew Brzezinski, Student Member, IEEE, and Eytan Modiano, Senior Member, IEEE, "Dynamic Reconfiguration and Routing Algorithms for IP-Over-WDM Networks With Stochastic Traffic".
15) Sinem Coleri Ergen and Pravin Varaiya, "Energy Efficient Routing with Delay Guarantee for Sensor Networks".
16) LAURA MARIE FEENEY, "An Energy Consumption Model for Performance Analysis of Routing Protocols for Mobile Ad Hoc Networks".
17) J.F. Kurose and K.W. Ross, "*Computer Networking—A Top-Down Approach Featuring the Internet"* Addison Wesley, 2003.
18) V.I. Levenshtein, "Binary Codes Capable of Correcting Deletions, Insertions, and Reversals" , *Soviet Physics Doklady*