International Journal of Wireless Communication
ISSN: 2231-3559 & E-ISSN: 2231-3567, Volume 2, Issue 1, 2012, pp.-29-34.
Available online at http://www.bioinfo.in/contents.php?id=109

A COMPETENT WAY TO DIMINISH THE BRUNT OF GRAY HOLE ATTACK IN MANET

DHAMANDE C.S. AND DESHMUKH H.R.

Dept. of CSE, B.N.C.O.E, Pusad, MS, India.
*Corresponding Author: Email- hrdphd@rediffmail.com, chetan.dhamande@gmail.com

Received: February 21, 2012; Accepted: March 15, 2012

Abstract- This paper analyzes the gray hole attack which is one of the possible attacks in ad hoc networks.In this we are mainly focus on the impact of gray hole attack on adhoc network & also find its consequences. An ad hoc network is a collection of mobile nodes that dynamically form a temporary network and are infrastructure less. The first is known as the" infrastructure network" (i.e. a network with fixed and wired gateways). The bridges for these networks are known as "base stations". A mobile unit within these networks connects to and communicates with the nearest base station that is within its communication radius. MANETs have some special characteristic features such as unreliable wireless links used for communication between hosts, constantly changing network topologies, limited bandwidth, battery power, low Computation power etc. Wireless networks can be basically either infrastructure based networks or infrastructure less networks. A gray hole may exhibit its malicious behavior 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. A variation of the black hole attack is the gray hole attack [1]. This attack when launched by the intermediate nodes selectively eaves drop the packets I.e. 50% of the packets, instead of forwarding all Another type of gray hole node may behave maliciously for Some time duration by dropping packets but may switch to normal behavior later.MANET contains diverse resources; the line of defence is very ambiguous; Nodes operate in shared wireless medium; Network topology changes unpredictably and very dynamically; Radio link reliability is an issue; connection breaks are pretty frequent. A gray hole may also exhibit a behavior which is a combination of the above two. The proposed technique is focus on the minimizing the impact of gray hole attack using AODV routing protocol .Simulation will be carried out using ns-2 tool.

Keywords- MANET, Gray Hole, AODV, Security, ns-2

Citation: Dhamande C.S. and Deshmukh H.R. (2012) A competent way to diminish the brunt of gray hole attack in Manet. International Journal of Wireless Communication, ISSN: 2231-3559 & E-ISSN: 2231-3567, Volume 2, Issue 1, pp.-29-34.

Introduction

MANET user can have better utilization of network resources only when it is connected to the Internet. But, global connectivity adds new security threats to the existing active and passive attacks on MANET. Security is an essential requirement in mobile ad hoc network (MANETs). Ad hoc network [2] is a wireless network without having any fixed infrastructure. A MANET is a collection of mobile nodes that can communicate with each other without the use of predefined infrastructure or centralized administration. MANET commercial applications have mainly been for military applications or emergency situations [3]. However ,we believe that research into MANET routing protocols will lay the groundwork for future wireless sensor networks and wireless plug-n-play devices MANETs have some special characteristic features such as unreliable wireless links used for communication between hosts, constantly changing network topologies, limited bandwidth, battery power, low computation power etc. Routing and network management are done cooperatively by each other nodes. Due to its dynamic nature MANET has larger security issues than conventional networks. We consider most common types of attacks on mobile ad hoc networks and on access point through which MANET is connected to the Internet. Specifically, we study how different attacks affect the performance of the network and find out the security issues which have not solved until now. The results enable us to minimize the attacks on integrated MANET-Internet communication efficiently. MANET user can have better utilization of network resources only when it is connected to the Internet. But, global connectivity adds new security threats to the existing active and passive attacks on MANET. Because we have to consider the attacks on access point also through which MANET is connected to Internet.Routing protocols are generally necessary for maintaining effective communication between distinct nodes. Routing protocol not only discovers network topology but also built the route for forwarding data packets and dynamically maintains routes between any pair of communicating nodes. The main goal of the security requirements for MANET is to provide a security protocol, which should meet the properties like confidentiality, integrity, availability and non-repudiation to the mobile users. In order to achieve this goal, the security approach should provide overall protection that spans the entire protocol stack.Routing protocols are designed to adapt frequent changes in the network due to mobility of nodes. The number of nodes in the network is not necessarily fixed. Every basic event consists of casually related protocol behavior and uses resources solely within a single node. It is easier to study the protocol behavior more accurately from the point of view of a single node. Specially, we study the basic routing behavior in MANET There are several issues in MANETS which addresses the areas such as IP addressing, radio interference, routing protocols, power Constraints, security, mobility management, bandwidth constraints, QOS, etc;. As of now some hot issues in MANETS can be related to the routing protocols, routing attacks, power and bandwidth constraints, and security, In AODV protocol, every mobile node maintains a routing table that stores the next hop node information for a route to a destination node. When a source node wishes to route a packet to a destination node, it uses the specified route if such a route is available in its routing table gray hole attack is one kind of routing disturbing attacks and can bring great damage to the network.AODV is a source initiated on-demand routing protocol. Every mobile node maintains a routing table that maintains the next hop node information for a route to the destination node. Because of open structure and limited battery-based energy some nodes (i.e. selfish or malicious) may not cooperate correctly. Detection of gray hole attack is harder because nodes can drop packets partially not only due to its malicious nature but also due to overload, In this paper we present a efficient way to detect the gray hole attack. The rest of the paper is organized as follows. In section 2, we discuss the related work on detection/removal of black hole & gray hole attacks. In section 3, we discuss the routing protocols for MANET. In section 4, we present the impact of gray hole attack on adhoc network. are discuss in section 5. Proposed work & objectives is discuss in section 5 finally the conclusion & discussion of future work is discussed in section 6.

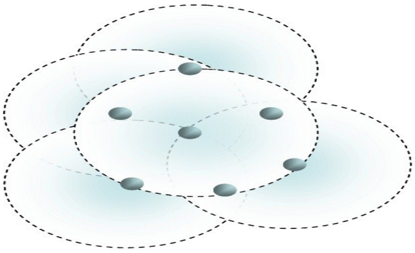

Fig. 1- Basic idea about adhoc network

Related Work

Security has become wide research area in MANETs. Secure ad hoc routing protocol has been proposed as a technique to enhance the security in MANET. The problem of security and cooperation enforcement has received considerable attention by researchers in the ad hoc network community. SCAN [3] exploits two ideas to protect the mobile ad hoc networks: 1) local collaboration: the neighboring nodes collectively monitor each other and sustain each other; and 2) information cross-validation: each node monitors its neighbors by cross-checking the overheard transmissions, and the monitoring results from different nodes are further cross validated. P. Agrawal et al [4] proposed a technique for detecting chain of cooperating malicious nodes (black and gray hole nodes) in ad hoc network. Gray Hole attack involving multiple malicious nodes. Gonzalez et al [5] presents a methodology, for detecting packet forwarding misbehavior, which is based on the principle of flow conservation in a network.Sukla Banerjee [6] have been suggested a scheme to detection & prevention of cooperative black/ gray hole attack in MANET. Mechanisms or technique to prevent the routing layer from malicious attacks for securing the system of a MANET by cryptographic techniques are proposed by Y. Hu, Perrig and Johnson [7], Papadimitratos and Hass [8], A detailed section on securing the AODV protocol is given in this publication. The first approach of securing the AODV protocol has been made by Zapata with his SAODV [9]. In a second publication [10] the protocol is presented in greater detail.

Routing protocols for MANET

MANET routing protocols can be categorized into different classes as: proactive,on reactive & hybrid.Routing protocols play crucial role in determining performance parameters such as packet delivery fraction, end to end (end 2 end) delay, packet loss etc. There are three types of routing protocols: Proactive Protocols, Reactive Protocols and Hybrid Protocols. Proactive protocols are table-driven that constantly update lists of destinations and routes. Reactive protocols respond on demand. Hybrid protocols combine the features of reactive and proactive protocols. The main goal of routing protocols is to minimize delay, maximize network throughput, maximize network lifetime and maximize energy efficiency of any ad hoc communication network. depending on the routing topology. Proactive protocols are. Examples of this type include Destination Sequence Distance Vector (DSDV). Reactive or source-initiated on-depending on the routing topology. Reactive or source-initiated on-demand protocols, in contrary, do not periodically update the routing information. It is propagated to the nodes only when necessary. Example of this type includes Dynamic Source Routing (DSR) and Ad Hoc On-Demand Distance Vector (AODV). Hybrid protocols make use of both reactive and proactive approaches. Example of this type includes Zone Routing Protocol (ZRP).

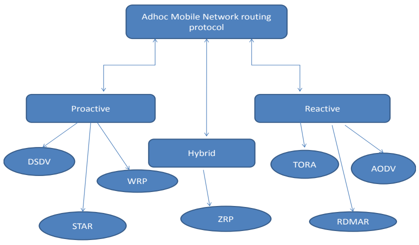

Fig. 2- Classification of MANET routing Protocol

AODV (Ad-hoc on-demand Distance Vector Routing)

The Ad hoc On-demand Distance Vector (AODV) is the widely used scalable protocol. But this shortest path algorithm prefers long hops, which results in routes with weak links. Hence route failure become frequent, even in case of less mobility, which degrades the network performance AODV is a source initiated on-demand routing protocol. Most of the existing MANET protocols optimize hop count as building a route selection. Examples of MANET protocols are Ad hoc On Demand Distance Vector (AODV) [11], Dynamic Source Routing (DSR)[12], and Destination Sequenced Distance Vector (DSDV) .Every mobile node maintains a routing table that maintains the next hop node information for a route to the destination node. When a Source node wishes to route a packet to a destination node, it uses the specified route if a fresh enough route to the destination node is available in its routing table. If not, it starts a route discovery process by broadcasting the Route Request (RREQ) message to its neighbours, which is further propagated until it reaches an intermediate node with a fresh enough route to the destination node specified in the RREQ, or the destination node itself. AODV builds routes using a route request / route reply query cycle. When a source node desires a route to a destination for which it does not already have a route, it broadcasts a route request (RREQ) packet across the network. Nodes receiving this packet update their information for the source node and set up backwards pointers to the source node in the route tables.AODV routing protocol is based on DSDV and DSR algorithm and is a state-of-the-art routing protocol that adopts a purely reactive strategy: it sets up a route on demand at the start of a communication session, and uses it till it breaks, after which a new route setup is initiated .AODV is a very simple, efficient, and effective routing protocol for Mobile Ad-hoc Networks which do not have fixed topology.AODV [13, 14] is an improvement of DSDV algorithm previously described. It is typically minimizes the number of required broadcasts by creating routes on a demand basis,The AODV protocol builds on the DSDV algorithm .it is an on demand routing algorithm. But in contrast to DSR it is a not source based routing scheme rather every hop of operation of the protocol is divided into two functions, route discovery & route maintenance. At first all the nodes send hello message on its interface and receive hello message from its neighbors. This process repeats periodically to determine neighbor connectivity .when a route is needed is to some destination, the protocols start route discovery .It uses two term route request & route reply.

DSR (Dynamic Source Routing)

The Dynamic Source Routing protocol (DSR) is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes. DSR allows the network to be completely self-organizing and self-configuring, without the need for any existing network infrastructure or administration. Network nodes (computers) cooperate to forward packets for each other to allow communication over multiple “hops” between nodes not directly within wireless transmission range of one another. As nodes in the network move about or join or leave the network, and as wireless transmission conditions such as sources of interference change, all routing is automatically determined and maintained by the DSR routing protocol The main feature of DSR is source routing in which the source always knows the complete route from source to destination. Route maintenance is used to monitor correctness of established route s & to initialize route discovery if a route fails.. The DSR protocol allows nodes to dynamically discover a source route across multiple network hops to any destination in the ad hoc network. In DSR, intermediate nodes do not need to preserve the routing information. Instead the packets themselves contain every routing decision Each data packet sent then carries in its header the complete, ordered list of nodes through which the packet must pass, allowing packet routing to be trivially loop-free 1and avoiding the need for up-to-date routing information in the intermediate nodes through which the packet is forwarded. By including this source route in the header of each data packet, other nodes forwarding or overhearing any of these packets may also easily cache this routing information for future use. The DSR protocol is composed of two mechanisms that work together to allow the discovery and maintenance of source routes in the ad hoc network: Route Discovery is the mechanism by which a node S wishing to send a packet to a destination node D obtains a source route to D. Route Discovery is used only when S attempts to send a packet to D and does not already know a route to D.

DSDV (Destination Sequenced Distance-Vector Routing Protocol)

In DSDV every node in the network maintains a routing table in which all of the possible destinations within the network and the number of hops to each destination are recorded. Each entry is marked with a sequence number assigned by the destination node. The sequence numbers enable the mobile nodes to distinguish stale routes from new ones, thereby avoiding the formation of routing loops. Routing table updates are periodically transmitted throughout the network in order to maintain table consistency. To help alleviate the potentially large amount of network traffic that such updates can generate, route updates can employ two possible types of packets: full dump and smaller incremental packets. Each of these broadcasts should fit into a standard-size of network protocol data unit (NPDU), thereby decreasing the amount of traffic generated. The mobile nodes maintain an additional table where they store the data sent in the incremental routing information packetsThe fundamental issue with DSDV is creation and maintenance of the tables. These tables need to be frequently updated by transmission of packets, even in traffic condition. Moreover, until updates about changes in topology are not sent across the network Destination-Sequenced Distance Vector (DSDV) is a traditional table-driven protocol for MANET. Nodes continuously update the tables to provide fresh view of whole network. Updates are so frequent that the advertisement must be made regularly enough to make sure that every node can almost always find every other node in the network. The main contribution of this algorithm was to solve the routing loop problem. In DSDV each node maintains a route to every other node in the network and thus routing table is formed. Each entry in the routing table contains sequence numbers which are even if a link is present; else, an odd number is used. The number is generated by the destination, and the emitter needs to send out the next update with this number. DSDV requires a regular update of its routing tables, which uses up battery power and a small amount of bandwidth even when the network is idle.

ZRP (Zone routing protocol)

The Zone Routing Protocol (ZRP) combines the advantages of the proactive and reactive approaches by maintaining an up-to-date topological map of a zone centered on each node an ad-hoc network, it can be assumed that the largest part of the traffic is directed to nearby nodes. Therefore, ZRP reduces the proactive scope to a zone centered on each node. In a limited zone, the maintenance of routing information is easier. Further, the amount of routing information that is never used is minimized.the Zone Routing Protocol, as its name implies, is based on the concept of zones. A routing zone is defined for Each node separately, and the zones of neighbouring nodes overlap. In ZRP, the knowledge of the local topology can be used for route maintenance. Link failures and sub-optimal route segments within one zone can be bypassed. Incoming packets can be directed around the broken link through an active multi-hop path. Similarly, the topology can be used to shorten routes, for example, when two nodes have moved within each other's radio coverage.ZRP comes under the hybrid protocol category. it uses the features of proactive & reactive routing protocol.

Gray Hole Attack

The main criterion for identification of a malicious node is the estimated percentage of packets dropped, which is compared against a pre-established misbehavior threshold. Any other node which drops packets in excess of the pre-established misbehavior threshold is said to be misbehaving, while for those nodes percentage of dropping packets is below the threshold are said to be properly behaving. A variation of this attack is the gray hole attack, in which nodes either drop packets selectively (e.g. dropping all UDP packets while forwarding TCP packets) or drop packets in a statistical manner (e.g. dropping 50% of the packets or dropping them with a probabilistic distribution). The gray hole attacks of this types will anyhow disrupt the network operation, if proper security measures are not used to detect them in place [15].One of these attacks is the Gray Hole attack. In the Gray Hole attack which lead to dropping of messages? Attacking node first agrees to forward packets and then fails to do so. Gray Hole attack may occur due to a malicious node which is deliberately misbehaving, as well as a damaged node interface.We first describe vulnerabilities in AODV protocol & then describe different types of gray hole attacks.In AODV protocol every node maintain a routing table that stores the next hop node information for a route a packet to destination node ,When a source node want to route a packet to the destination node , it uses a specific route if such a route is available in it's routing table.otherwise , nodes initiates a route discovery process by broadcasting Route Request (RREQ) message to it's neighbours. On receiving RREQ message, the intermediate nodes update their routing tables for a reverse route to source node.A Route Reply (RREP) message is sent back to the source node when the RREQ query reaches either the destination node itself or any other node that has a current route to destination.We now describe the gray hole attack on MANET'S .The gray hole attack has two phases , In first phase, a mallicious node exploits the AODV protocol to advertise itself as having a valid route to destination node, with the intension of interupting or corrupting packets, event though route is spurious.In second phase ,nodes drops the interupted packets with a certation probability. To detect black and gray hole nodes, one proposal is having the sender occasionally check through all available routes to determine if the destination received all of its messages intact. In order to circumvent any gray hole nodes that might interfere with message traffic, the sender broadcasts a "check" request message (Fig. 3), For example, source node S wants to send data packets to destination node D and initiates the route discovery process. We assume that node 2 is a malicious node and it claims that it has route to the destination whenever it receives route request packets, and immediately sends the response to node S. If the response from the node 2 reaches first to node S then node S thinks that the route discovery is complete, ignores all other reply messages and begins to send data packets to node 2. As a result, all packets through the malicious node are consumed or lost.In Gray Hole Attack a malicious node refuses to forward certain packets and simply drops them. The attacker selectively drops the packets originating from a single IP address or a range of IP addresses and forwards the remaining packets. Gray Hole nodes in MANETs are very effective. The simulation results will show that the mechanism is effective and efficient.

In below figure

- S-Source
- D-Destination
- 1-Node1, 3-Node3
- 2-Malicious Node, 4-Node4

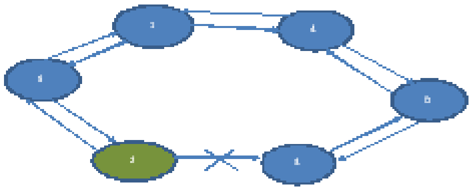

Fig. 3- Gray Hole Attack in MANET

Security Attacks

The security attacks in MANET can be roughly classified into two major categories, namely passive attacks and active attacks.

- **Active attack***:* 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.
- **Passive attack***:* 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 [16] 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, thereby making it impossible for the attacker to get useful information from the data overhead.

Examples of security attacks

- **Wormhole attack**

Wormhole attacks [17,18] are severe threats to MANET routing protocols. The wormhole attack is particularly dangerous against many ad hoc network routing protocols in which the nodes that hear a packet transmission directly from some node consider e of (and thus a neighbour of) that node.In a wormhole attack, an attacker receives packets at one point in the network, “tunnels” them to another point in the network, and then replays them into the network from that point. For tunnelled distances longer than the normal wireless transmission range of a single hop, it is simple for the attacker to make the tunnelled packet arrive with better metric than anormal multihop route.

- **Sinkhole attack**

The attacking node tries to offer a very attractive link e.g. to a gateway. Therefore, a lot of traffic bypasses this node. Besides simple traffic analysis other attacks like selective forwarding or denial of service can be combined with the sinkhole attack.

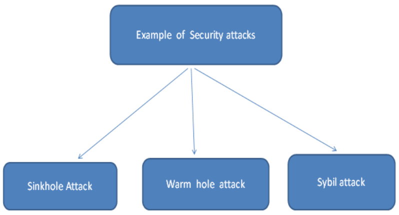

Fig. 4- Example of security attack

Proposed Methodology

Objectives

Objectives of this proposed work are summarized as follow

To compare effects of normal AODV & Gray Hole attack in the term of Network load, packet delivery ratio and End to End delay, packet loss ratio in MANET and also find the performance of the adhoc network.

Use the ns-2 as a simulator to simulate gray hole attack .

Comparing the results of AODV protocol with and without Gray Hole attack.

Implement new security method using AODV as a counter measure of gray hole attack & also minimize the effect of gray hole attack and improves the reliability as well as effectiveness of the adhoc network.

Planned Work

a) Segment 1: Realization of AODV

This segment mainly deals with the implementation aspect of AODV protocol and performance metrics is also taken into the account.

b) Segment 2: Realization of gray hole attack

In this module, implementation of gray hole attack in MANET & it’s consequences is taken into consideration & it is going to split into three way RREQ,RREP & Route error msg.

Segment 3: Realization Of security method for gray hole attack

In this segment a proposed security method is going to be realized which is mainly focus on the minimizing the effect of gray hole attack in MANET & provide the safety to the adhoc network.

New way to handle the malicious node in MANET

The main idea about this method is to find out the malicious node in the adhoc network and minimize as well as removed the malicious node from the network area and improves the network performance. Final step is to make the adhoc network as secure from the routing attacks. This method involves the different parameters such as

- Adhoc network
- NI – Node ID,
- DSN – Destination Sequence Number,
- MID– Malicious Node ID.
- RR- Request Reply Table

Phase 1: Start the process to handle the malicious node
Add the current time status
Add the current time status with waiting time (WT)

Phase 2: storage phase of the Process
Store all the Route Replies DSN and NI in RR-Table
Repeat the above process until the time exceeds.

Phase 3: Recognize phase of malicious node
Access the first entry from RR-Table
If DSN is much greater than SSN then discard entry from RR-Table and store its NI in MID.

Phase 4: Selecting phase of node
Manage and sort the contents of RR-Table entries according to the DSN, Select the NI having highest DSN among RR-table entries.

Phase 5: Carry on with Default phase Process
Start Malicious Node handle procedure for AODV Protocol the above procedure starts from the starting process, first set the waiting time for the source node SSN to receive the RREQ coming from other nodes and then add the current time with the waiting time. Then in storing process, store all the RREQ Destination Sequence Number (DSN) and its Node ID ie NI n RR-Table until the computed time exceeds. Generally the first route reply will be from the malicious node with high destination sequence number, which is stored as the first entry in the RR-Table. Then match the first destination sequence number DSN with the source node sequence number SSN, if there exists much more differences between them, surely that node is the malicious node, immediately remove that entry from the RR-Table. This is how malicious node is recognized and removed. Final process is selecting the next node id that has the higher destination sequence number, is obtained by sorting the RR-Table according to the DSEQ-NO column, whose packet is sent to malicious node recognition in order to carry on the default operations of AODV protocol.

Conclusion and Future Work

In this paper we have studied the brunt of the gray hole attack in adhoc network. Gray hole attack ultimately decrease the concert of the network & also shady the data Proposed solution is mainly focus on the diminish the impact of gray hole attack in MANET & also improve the security as well as the performance of the network.

References

[1] Oscar F. Gonzalez, God win Ansa, Michael Howarth and George Pavlou., *Journal of Internet.*

[2] Poongothai T. and Jayarajan K. (2008) *International Conference of Computing, Communication and Networking*, 18-20, VI, 1-4.

[3] Yang H., Shu J., Meng X. and Lu S. (2006) *IEEE Journal on Selected Areas in Communications*, 24(2), 261-273.

[4] Bo Sun, Yong Guan, Jian Chen (2003) *IEEE.*

[5] Piyush Agrawal, Ghosh R.K., Sajal K. Das (2008) *The 2nd international conference on Ubiquitous information management and communication*, 310-314.

[6] Sukla Banerjee (2008) *The World Congress on Engineering and Computer Science*.

[7] Hu Y., Perrig A. and Johnson D. (2002) *The 8th Annual International Conference on Mobile Computing and Networking*, 12 -23.

[8] Papadimitratos P. and Haas Z. (2002) *SCS Communications Networks and Distributed Systems Modeling and Simulation Conference*.

[9] Zapata M.G. (2001) *Secure ad-hoc on-demand distance vector (saodv) routing.*

[10] Perkins. C.E. and Bhagwat P. (1994) *ACM*, 234-244.

[11] Perkins C.E. and Royer E.M. (1999) *IEEE Workshop on Mobile. Comp. Systems .and Applications*, 90-100.

[12] Johnson D.B. and Maltz D.A. (1996) *Mobile Computing*, 153-181.

[13] Perkins C.E. and Bhagwat P. (1994) *ACM SIGCOMM 94*, 234 -244.

[14] Vishnu K. and Amos J. Paul (2010) *International Journal of Computer Applications*,1(22), 38-42.

[15] Misra P. (2006) *Routing Protocols for Ad Hoc Mob. Wireless Networks.*

[16] Madhu Viswanatham V. and Chari A.A. (2008) *Journal of Computer Science,* 4(3), 245-251.

[17] Hu Y.C., Perrig A. and Johnson D.B. (2003) *22 Annual joint Conf. IEEE Computer and Communication Societies*.

[18] Nait-Abdesselam F., Bensaou B. and Taleb T. (2003) *IEEE Communicat Magaz*, 46(4), 127-33.