Attacks and Corresponding Solutions in MANETS

Tadanki Vasavi[1], *Mrs. Y. Adilakshmi*[2],

[1]*M.Tech, CSE Dept, Gudlavalleru Engineering College, Gudlavalleru, India*

[2]*Associate Professor, CSE Dept, Gudlavalleru Engineering College, Gudlavalleru, India*

Abstract: *Security may be a major concern for protected communication between mobile nodes in a very hostile surroundings. In hostile environments adversaries will bunch active and passive attacks against intercept in a position routing in plant in routing message and knowledge packets. During this paper, we tend to specialize in basic security attacks in Mobile adhoc networks. Manet has no clear line of defense, so, it's accessible to each legitimate network users and malicious attackers. within the presence of malicious nodes, one in every of the most challenges in Manet is to style the sturdy security answer that may defend Manet from numerous routing attacks. However, these answer don't seem to be appropriate for Manet resource constraints, i.e., restricted information measure and battery power, as a result of they introduce significant traffic load to exchange and collateral keys. Manet will operate in isolation or in coordination with a wired infrastructure, usually through a entryway node taking part in each networks for traffic relay. This flexibility, in conjunction with their self-organizing capabilities, is a few of MANET's biggest strengths, still as their biggest security weaknesses. During this paper completely different routing attacks, like active (flooding, black hole, spoofing, and wormhole) and passive (eavesdropping, traffic observation, and traffic analysis) area unit represented.*

I. Introduction:

Mobile accidental Networks (MANETs) has become one in every of the foremost current areas of analysis within the recent years attributable to the challenges it cause to the connected protocols. Manet is that the new rising technology that allows users to speak with none physical infrastructure despite their geographical location, that's why it's typically brought up as associate "infrastructure less" network. The proliferation of cheaper, tiny and a lot of powerful devices build Manet a quickest growing network. associate adhoc network is self organizing and adjectives. Device in mobile accidental network ought to be ready to observe the presence of different devices and perform necessary originated to facilitate communication and sharing of knowledge and repair. accidental networking permits the devices to take care of connections to the network additionally as simply adding and removing devices to and from the network. The set of applications for MANETs is various, starting from large-scale, mobile, extremely dynamic networks, to small, static networks that square measure forced by power sources. Besides the inheritance applications that move from ancient infrastructure setting into the accidental context, a good deal of recent services will and can be generated for the new setting. It includes:

1. Military Battlefield
2. Sensor Networks
3. Medical Service
4. Personal Area Network

Security arrangements are vital issues for MANET, particularly for those choosing touchy applications, need to meet the accompanying plan objectives while tending to the above difficulties. MANET is more helpless than wired system because of portable hubs, dangers from traded off hubs inside the system, restricted physical security, dynamic topology,

adaptability and absence of brought together administration. As a result of these vulnerabilities, MANET is more inclined to vindictive assaults. The essential focal point of this work is to give a review on different kinds of assaults that influence the MANET conduct because of any reason.

I. Characteristics of MANET:

Distributed operation: There is no foundation organize for the focal control of the system tasks, the control of the system is dispersed among the hubs. The hubs associated with a MANET ought to participate with one another and convey among themselves and every hub goes about as a transfer as required, to actualize particular capacities, for example, steering and security.

Multi hop routing: At the point when a hub attempts to send data to different hubs which is out of its correspondence go, the parcel ought to be sent by means of at least one middle of the road hubs.

Autonomous terminal: In MANET, every portable hub is an autonomous hub, which could work as both a host and a switch.

Dynamic topology: Hubs are allowed to move self-assertively with various velocities; in this way, the system topology may change haphazardly and at erratic time. The hubs in the MANET progressively build up directing among themselves as they travel around, setting up their own system.

Light-weight terminals: In most extreme cases, the hubs at MANET are versatile with less CPU capacity, low power stockpiling and little memory measure.

Shared Physical Medium: The remote correspondence medium is available to any substance with the suitable gear and satisfactory assets. As needs be, access to the channel can't be confined.

II. MANET Challenges:

Limited bandwidth: Remote connection keep on having altogether bring down limit than infrastructured systems. Also, the acknowledged throughput of remote correspondence in the wake of representing the impact of different access, blurring, commotion, and obstruction conditions, and so on., is frequently substantially less than a radio's greatest transmission rate.

Dynamic topology: Dynamic topology enrollment may irritate the trust relationship among hubs. The trust may likewise be bothered if a few hubs are recognized as traded off.

Routing Overhead: In remote adhoc systems, hubs frequently change their area inside system. In this way, some stale courses are produced in the directing table which prompts superfluous steering overhead.

Hidden terminal problem: The concealed terminal issue alludes to the impact of bundles at an accepting hub because of the concurrent transmission of those hubs that are not inside the immediate transmission scope of the sender, yet are inside the transmission scope of the beneficiary.

Packet losses due to transmission errors: Impromptu remote systems encounters a considerably higher bundle misfortune because of variables, for example, expanded impacts because of the nearness of shrouded terminals, nearness of obstruction, uni-directional connections, visit way breaks because of portability of hubs.

Mobility-induced route changes: The system topology in an impromptu remote system is exceedingly unique because of the development of hubs; thus an on-going session endures visit way breaks. This circumstance regularly prompts visit course changes.

Battery constraints: Gadgets utilized in these systems have limitations on the power source so as to look after transportability, size and weight of the gadget.

Security threats: The wireless mobile ad hoc nature of MANETs brings new security challenges to the network design. As the wireless medium is vulnerable to eavesdropping and ad hoc network functionality is established through node cooperation, mobile ad hoc networks are intrinsically exposed to numerous security attacks.

II. MANETs Applications:

Some of the typical applications include:

Military battlefield: Ad-Hoc networking would allow the military to take advantage of commonplace network technology to maintain an information network between the soldiers, vehicles, and military information head quarter.

Collaborative work: For some business environments, the need for collaborative computing might be more important outside office environments than inside and where people do need to have outside meetings to cooperate and exchange information on a given project.

Local level: Ad-Hoc networks can autonomously link an instant and temporary multimedia network using notebook computers to spread and share information among participants at a e.g. conference or classroom. Another appropriate local level application might be in home networks where devices can communicate directly to exchange information.

Personal area network and Bluetooth: A personal area network is a short range, localized network where nodes are usually associated with a given person. Short-range MANET such as Bluetooth can simplify the inter communication between various mobile devices such as a laptop, and a mobile phone.

Commercial Sector: Ad hoc can be used in emergency/rescue operations for disaster relief efforts, e.g. in fire, flood, or earthquake. Emergency rescue operations must take place where non-existing or damaged communications infrastructure and rapid deployment of a communication network is needed.

III. Related Work:

A MANET is a most encouraging and quickly developing innovation which depends on a self-composed and quickly conveyed system. Because of its awesome highlights, MANET draws in various genuine application territories where the systems topology changes rapidly. Be that as it may, in numerous specialists are attempting to expel principle shortcomings of MANET, for example, restricted data transmission, battery control, computational power, and security. The current security arrangements of wired systems can't be connected straightforwardly to MANET, which makes a MANET significantly more powerless against security assaults. In this paper, we have talked about current directing assaults in MANET. A few arrangements that depend on cryptography and key administration appear to be encouraging, however they are excessively costly for asset compelled in MANET. They still not immaculate as far as tradeoffs among adequacy and productivity. A few arrangements in function admirably within the sight of one vindictive hub, they probably won't be material within the sight of numerous plotting assailants. What's more, some may require extraordinary equipment, for example, a GPS or a change to the current convention.

The malevolent node(s) can assaults in MANET utilizing diverse courses, for example, sending counterfeit messages a few times, counterfeit steering data, and promoting counterfeit connects to upset directing activities. In the accompanying subsection, current directing assaults and its countermeasures against MANET conventions are talked about in detail.

IV. MANET Vulnerabilities:

Defenselessness is a shortcoming in security framework. A specific framework might be defenseless against unapproved information control on the grounds that the framework does not confirm a client's personality previously permitting information get to. MANET is more helpless than wired system. Some of the vulnerabilities are as follows:-

Lack of centralized management: MANET doesn't have a unified screen server. The nonappearance of administration makes the recognition of assaults troublesome in light of the fact that it isn't east to screen the activity in a very powerful and substantial scale adhoc arrange. Absence of brought together administration will block trust administration for hubs.

Resource availability: Asset accessibility is a noteworthy issue in MANET. Giving secure correspondence in such changing condition and in addition insurance against particular dangers and assaults, prompts improvement of different security plans and structures. Synergistic specially appointed situations likewise permit usage of self-sorted out security component.

Scalability: Because of portability of hubs, size of specially appointed system changing constantly. So versatility is a noteworthy issue concerning security. Security system ought to be equipped for taking care of an extensive system and in addition little ones.

Cooperativeness: Steering calculation for MANETs for the most part expect that hubs are agreeable and non-malignant. Thus a malevolent aggressor can without much of a stretch turn into a critical directing specialist and upset system task by defying the convention details.

Dynamic topology: Dynamic topology and variable hubs participation may irritate the trust relationship among hubs. The trust may likewise be aggravated if a few hubs are distinguished as bargained. This dynamic conduct could be better ensured with disseminated and versatile security instruments.

Limited power supply: Dynamic topology and variable hubs participation may exasperate the trust relationship among hubs. The trust may likewise be aggravated if a few hubs are recognized as traded off. This dynamic conduct could be better ensured with conveyed and versatile security instruments.

V. Security Goals:

Security includes an arrangement of speculations that are satisfactorily subsidized. In MANET, all systems administration capacities, for example, steering and parcel sending, are performed by hubs themselves in a self arranging way. Consequently, anchoring a portable adhoc organize is exceptionally testing. The objectives to assess if portable adhoc organize is secure or not are as follows:

Availability: Accessibility implies the benefits are available to approved gatherings at proper occasions. Accessibility applies both to information and to administrations. It guarantees the survivability of system benefit in spite of refusal of administration assault.

Confidentiality: Secrecy guarantees that PC related resources are gotten to just by approved gatherings. That is just the individuals who ought to approach something will really get that entrance. To keep up classification of some private data, we have to keep

them mystery from all elements that don't have benefit to get to them. Classification is here and there called mystery or protection.

Integrity: Respectability implies that advantages can be changed just by approved gatherings or just in approved way. Adjustment incorporates composing, evolving status, erasing and making. Respectability guarantees that a message being exchanged is never defiled.

Authentication: Confirmation empowers a hub to guarantee the personality of companion hub it is speaking with. Validation is basically confirmation that members in correspondence are verified and not impersonators. Credibility is guaranteed in light of the fact that just the authentic sender can deliver a message that will decode appropriately with the mutual key.

Nonrepudiation: Nonrepudiation guarantees that sender and recipient of a message can't repudiate that they have ever sent or got such a message .This is useful when we have to separate if a hub with some undesired capacity is endangered or not.

Anonymity: Anonymity means all data that can be utilized to recognize proprietor or current client of hub should default be kept private and not be circulated by hub itself or the framework programming.

VI. Security Attacks:

Securing wireless adhoc networks is a profoundly difficult issue. Understanding conceivable type of assaults is dependably the initial move towards growing great security arrangements. Security of correspondence in MANET is imperative for secure transmission of data. Nonattendance of any focal coordination system and shared remote medium makes MANET more defenseless against advanced/digital assaults than wired system there are various assaults that influence MANET. These attacks can be classified into two types:

- **Active Attacks**
- **Passive Attacks**

Active Attacks: Active attacks these are the assaults that are performed by the pernicious hubs that bear some vitality cost with the end goal to play out the assaults. Dynamic assaults include some alteration of information stream or production of false stream. Dynamic assaults can be inward or outside. Outer assaults are completed by hubs that don't have a place with the system. Inward assaults are from traded off hubs that are a piece of the system. Since the aggressor is as of now part of the system, inner assaults are more serious and difficult to recognize than outside assaults. Dynamic assaults, regardless of whether completed by an outer warning or an inner bargained hub includes activities, for example, pantomime (disguising or caricaturing), alteration, manufacture and replication.

a. Black Hole Attack: In “Black Hole Attack” it is a malevolent hub abuses the vulnerabilities of course revelation methodology of a receptive directing convention. The noxious hub as a middle of the road hub on receipt of a RREQ message sends a RREP with the goal arrangement number bigger than is in the RREQ message demonstrating that it has a crisp course to the goal. This RREP from malevolent hub will achieve source hub before the answer send by goal/real middle of the road hub. The source hub will in this way select the course which goes through pernicious hub. By rehashing this for RREQs got from different sources the pernicious hub catches a few courses pulling in the information movement from all sources towards it consequently making a dark gap in the system. The pernicious hub would then be able to abuse or dispose of the activity. The Fig. 1 demonstrates the malignant hub (MN) sending counterfeit RREPs to two sources in the

system and catching the courses of both the sources consequently making a Black opening.

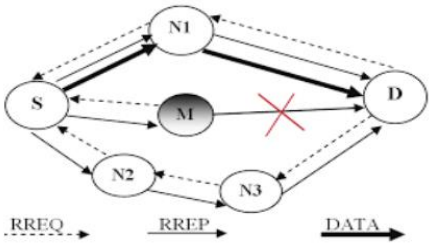

Fig.1 Black Hole Attack

b. Gray Hole Attack: In "Grey Hole Attack", the malicious node first catches the course as in Black gap assault by misusing the vulnerabilities of course disclosure procedure of the steering conventions and afterward it drops the blocked bundles with a specific likelihood. The vindictive hub in this kind of assault may drop bundles originating from certain particular hubs while sending every one of the parcels for different hubs or it might drop parcels for quite a while and carry on regularly for rest of the time or a blend of the over two, along these lines making identification of noxious hub extremely troublesome. Fig. 2 demonstrates the Gray Hole Node (GHN) drop the bundles originating from the objective hub.

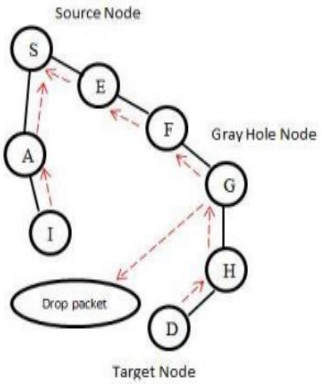

Fig.2 Gray Hole Attack

c. Rushing Attack: In "Rushing Attack" the malicious node rushes i.e. transport prior the RREQ message to its neighbors in this manner stifling the rebroadcast from genuine hubs. In the receptive directing conventions a transitional hub reacts just to the primary RREQ message which is gotten and stifles other copy RREQ bundles by the utilization of the source succession numbers. The noxious hub transmits the RREQ message sooner than all around carried on hubs by either evacuating the defers which the message needs to endure at the MAC layer or by utilizing long range remote transmission. As the RREQ just goes through malevolent hub, it mediates itself in the chose course and from that point causes authentic information bundles to be directed in useless way.

d. Wormhole Attack: "Wormhole attack" is propelled by a two or more conniving noxious hubs which catches the parcel at one area, transports it over the passage to the next area and replays at the separation area bypassing the middle of the road hub. The passage so made gives a feeling that the two hubs are one bounce away and accordingly gives the most brief way to the goal. The match of intriguing malignant hub makes movement stifle focuses which are under the control of aggressors and can be used to dispatch the dynamic or aloof assaults. The passage can be set up by either In-Band Channel or Out-Band Channel. In Out-Band Channel the intriguing hubs set up an immediate connection between the two plotting hubs by long range remote transmission or by a private rapid system. Despite what might be expected, the In-band channel does not utilize the outside correspondence medium to make the passage; rather it utilizes embodiment to build up a secretive overlay burrow

over the current remote medium. A wormhole assault is similarly hazardous for both proactive and receptive steering conventions. It is conceivable regardless of whether all correspondences give realness and classification. Fig 3 indicates MN1 and MN2 making hallucination of being neighbors by exemplification to build up an incognito overlay burrow over the current remote medium. It sends bogus commercial of 1-bounce connect somewhere in the range of MN1 and MN2 without the genuine trade of Hello messages.

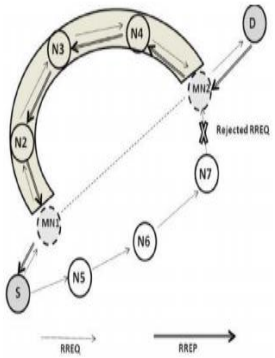

Fig.3 Worm hole Attack

e. Sybil attack: The Sybil assault particularly goes for appropriated framework situations. The aggressor endeavors to go about as a few distinct personalities/hubs instead of one. This enables him to produce the aftereffect of a casting a ballot utilized for limit security strategies. Since impromptu systems rely upon the correspondence between hubs, numerous frameworks apply excess calculations to guarantee that the information gets from source to goal. A result of this is aggressors have a harder time to wreck the honesty of data.

f. Flooding Attack: Malicious nodes may likewise infuse false bundles into the system, or make phantom parcels which circle around because of false steering data, adequately spending the transfer speed and preparing assets en route. This has particularly genuine impacts on specially appointed systems, since the hubs of these normally have just restricted assets regarding battery and computational power. Movement may likewise be a money related factor, contingent upon the administrations gave, so any flooding which explodes the activity measurements of the system or a specific hub can prompt impressive harm cost.

Passive Attacks: Passive attacks are the attack does not disturb appropriate activity of network. Attackers snoop information traded in system without changing it. Prerequisite of privacy can be abused if an assailant is likewise ready to decipher information accumulated through snooping.Detection of these assault is troublesome since the activity of system itself does not get influenced.

a. Traffic Monitoring: It tends to be produced to distinguish the correspondence gatherings and usefulness which could give data to dispatch additionally assaults .It isn't particular to MANET, different remote system, for example, cell, satellite and WLAN likewise experience the ill effects of these potential vulnerabilities.

b. Eavesdropping: The term listens stealthily infers catching without consuming any using any additional exertion. In this blocking and perusing and discussion of message by unintended recipient occur. Portable host in versatile specially appointed system shares a remote medium. Larger parts of remote correspondence utilize RF range and communicated ordinarily. Message transmitted can be listened stealthily and counterfeit message can be infused into system.

c. Traffic Analysis: Traffic analysis is an inactive assault used to pick up data on which hubs speak with one another and how much information is prepared.

d. Syn flooding: This attack is denial of service attack. An assailant may over and over make new association ask for until the point that the assets required by every association are depleted or achieve a greatest cutoff. It produces extreme asset requirements for authentic hubs.

TABLE 1: SUMMARY OF ATTACKS AND THEIR COUNTERMEASURES

Sr. No.	Types of attacks and Routing Protocol Vulnerabilities	Suggested Countermeasures	Advantages/Disadvantages of the Scheme
1.	**Black Hole Attack** • The Malicious node interposes between source nodes and destination nodes. • Intermediate malicious node sends fake RREP. Manipulates Destination Sequence number and hop count. Attracts data traffic towards itself. • It discards data traffic and prevents from reaching destination. Most effective against reactive routing protocols, viz. AODV & DSR	• "Chavda, K." in [13] proposes Comparison of Destination Sequence numbers of at least two RREPs. • Detection of malicious node if destination sequence number is arbitrarily high. • "Abdelhaq, M." in [14] proposes Local Intrusion Detection (LID) security mechanism. • RREP from the intermediate node is checked by immediately previous node by sending a FRREQ message to the next node.	• Simple and minimum overheads. • Unable to isolate the malicious node if it does not use arbitrary high destination number. • An improvement over the earlier scheme Source Intrusion Detection(SID) Mechanism. • More complex.
2.	**Grey Hole Attack** • Malicious node exploits same vulnerabilities as in Black Hole Attack.It exhibits malicious behavior in different ways. May discard data traffic of specific nodes while behaving normally for other nodes or may discard data traffic for some time and behave normally for rest of the time or a combination of the above two.	• "Sen, J." in [6] proposes, monitoring and analysis of the behavior of neighboring nodes with respect to data traffic. The malicious nodes are detected if traffic pattern does not conform to lay down rules.	• Significant high detection rate with moderate traffic overheads.
3.	**Rushing Attack** • Malicious node rushes the RREQ message to its neighbors thus suppressing the rebroadcast of RREQ from legitimate nodes. • Malicious node rushes the RREQ message by either removing the delays which the message has to suffer at the MAC layer or by transmitting using long range wireless transmission. • Malicious node interposes itself in the selected route and thereafter causes legitimate data packets to be routed in dysfunctional manner.	• "Hu, Y." in [17] proposes Secure Neighbor Detection, Secure Route Delegation, and Randomized RREQ forwarding. • Secure Neighbor Detection allows each neighbor to verify that the other is within a given maximum transmission range. • The Randomized Selection of RREQ message to be forwarded, replaces traditional duplicate suppression in on demand route discovery.	• It will require extra hardware to determine the location of nodes using GPS or synchronized clock.
4	**Wormhole Attack** Two or more colluding malicious nodes captures the traffic at one end replays at the distance location bypassing the intermediate nodes. The malicious nodes create a tunnel to give an impression that the two nodes are one hop away and thus provide the shortest path to the destination. • The tunnel can be established by either In-Band Channel or Out-Band Channel. • The pair of colluding malicious	• "Hu, Y." in [18] has proposed Temporal and geographical Packet Leaches to protect against the attack. • "Mary, E." in [8] has proposed Wormhole Secure Routing using certificate chaining has been proposed. • The protocol uses round trip time (RTT) between nodes to issue • certificates to the legitimate nodes. • "Mahajan, V." in [19] proposes a technique that exploits the anomaly in the network behavior for in-band wormhole attack in proactive protocol.	• Require extra hardware in terms of GPS / tightly synchronizes clock. • The technique may give false alarm due to variations in the RTT. • Detection with moderate traffic overheads.

	node creates traffic choke points which can be utilized to launch the active or passive attacks. • It is equally dangerous for both proactive and reactive routing protocols. It is possible even if communications provide authenticity and confidentiality.	• The anomalies in the path length and in incompatible hop delays and end-to-end delay have been used to detect Wormhole.	
5	**Sybil Attack** Malicious node creates and controls multiple identities. Exploits vulnerability of absence of any centralized identity management mechanism. • Malicious node can either create a new identity after discarding the previously created identity or can create several identities simultaneously with the aim to cause disruption in the network. • The Sybil attack can affect both proactive and reactive routing protocols.	• "Abbas, S." in [10] has proposed, Distributed technique for Sybil attack detection when attacker concurrently uses all the identities. • Movement of all the identities when the node moves in the network is captured. • Identities travelling the same path are considered Sybil identities. • "Kesidis, S." in [7] has proposed, a technique which utilizes received signal strength in order to differentiate legitimate and Sybil nodes. • The entry and exit behavior of the nodes is analyzed and is compared against a threshold.	• GPS for location determination and directional antenna are required • Light weight technique with low traffic overheads. No extra specialized hardware like directional antennas, GPS and centralized TTP required.
6	**Flooding attack** • A malicious node can flood the network with route request to the nonexistent or arbitrary destinations. • The purpose is to unnecessarily use bandwidth, computational resources, memory resources, power resources, and prevents the normal operation of the routing-protocol. Broadcast of RREQ in Reactive routing protocols and TC control messages in Proactive routing protocols.	• "Zhang, S" in [20] has proposed a technique in which each node monitors its neighbors' RREQ and if rate exceeds the predefined threshold, the node is declared as malicious. • "Desilva, S." in [21] has proposed an improvement to fixed threshold for deciding the malicious behavior of flooding node. • The proposed technique is an adaptive technique based on statistical analysis to decide the threshold for declaring a malicious node.	• Attack goes unnoticed below the fixed threshold. • Legitimate node may get blacklisted if identity is impersonated by malicious node. • Reduces the impact of the attack for varying flooding rates.

VII. Conclusion:

An attempt has been made to exhibit a review of all the current security assaults in the MANET. There is a need to make them more secure and vigorous to adjust to the requesting necessities of these system. This paper presumes that exploration on MANET security is as yet a testing issue and it opens the entryway for analysts.

REFERENCES:

1] Y.C. Hu, A. Perrig, D.B. Johnson, Rushing attacks and defense in wireless ad hoc network routing protocols, in Proceedings of ACM WiSe 2003, San Diego, CA, September 2003.
[2] I. Aad, J.P. Hubaux, E.W. Knightly, Denial of service resilience in ad hoc networks, in: Proceedings of ACM MobiCom 2004, Philadelphia, PA, September 2004.
[3] Y.C. Hu, A. Perrig, D.B. Johnson, Ariadne: A secure ondemand routing protocol for ad hoc networks, in: Proceedings of ACM MobiCom 2002, Atlanta, Georgia, September 2002.
[4] S.J. Lee, W. Su, M. Gerla, On-Demand Multicast Routing Protocol in Multihop Wireless Mobile Networks, ACM/ Kluwer Mobile Networks and Applications 7 (6) (2002) 441– 453.
[5] J.J. Garcia-Luna-Aceves, E.L. Madruga, The Core-Assisted Mesh Protocol, IEEE Journal on Selected Areas in Communications 17 (8) (1999) 1380–1994.
[6] S.K. Das, B.S. Manoj, C. Siva Ram Murthy, A dynamic core-based multicast routing protocol for ad hoc wireless networks, in: Proceedings of ACM MOBIHOC 2002, June 2002, pp. 24–35.

[7] S. Lee, C. Kim, Neighbor supporting ad hoc multicast routing protocol, in: Proceedings of ACM MOBIHOC 2000, August 2000, pp. 37–50.
[8] E.M. Royer, C.E. Perkins, Multicast operation of the ad hoc on-demand distance vector routing protocol, in: Proceedings of MobiCom'99, Seattle, WA, August 1999.
[9] C.W. Wu, Y.C. Tay, C.K. Toh, Ad hoc multicast routing protocol utilizing increasing id-numbers (amris) functional specification, Internet draft, work in progress, draft-ietfmanet- amris-spec-00.txt, November 1998.
[10] C.E. Perkins, E.M. Royer, S.R. Das, Ad hoc on demand distance vector (AODV) routing, in: Proceedings of IEEE WMCSA'99, New Orleans, LA, February 1999.
[11] B. Awerbuch, D. Holmer, C. Nita-Rotaru, H. Rubens, An on-demand secure routing protocol resilient to byzantine failures, in: Proceedings of ACM WiSe 2002, Atlanta, Georgia, September 2002.
[12] C.E. Perkins, P. Bhagwat, Highly dynamic destinationsequenced distance-vector routing (DSDV) for mobile computers, in: Proceedings of ACM SIGCOMM'94, August 1994.
[13] D.B. Johnson, D.A. Maltz, Y.C. Hu, J.G. Jetcheva, Dynamic Source Routing in Ad Hoc Wireless Networks, Mobile Computing, vol. 5, Kluwer Academic Publishers., 1996, pp. 153–181.
[14] QualNet Simulator, Available from: <http://www.qualnet.com>.
[15] V. Gupta, S. Krishnamurthy, M. Faloutsos, Denial of service attacks at the MAC layer in wireless ad hoc networks, in: Proceedings of IEEE MILCOM'02, 2002.