A Comprehensive Appraisal of Ad hoc Networks

Amandeep Verma
Lecturer in Computer Science,
Punjabi University Regional Centre Mohali

Manpreet Singh Gujral
Department of Computer Engineering,
University College of Engineering,
Punjabi University, Patiala

ABSTRACT
An ad hoc network is a group of wireless mobile hosts that are connected momentarily through wireless connections in the dearth of any centralized control or some supporting services. The circumstances where it is likely unrealistic or infeasible to deploy infrastructure, in these cases mobile devices could set up a possibly short lived network for the communication needs of the moment by a quick deployment. Security is a vital issue in an ad hoc network owing to its intrinsic vulnerabilities. These vulnerabilities are nature of its structure that cannot be eliminated. Consequently, attacks with malicious objectives have been and will be devised to exploit these vulnerabilities and to perturb its operations. This paper presents an inclusive study of the ad hoc network in terms of its characteristics, vulnerabilities, challenges, routing, authentication and attacks specific to these types of networks.

Keywords
ad hoc networks, vulnerabilities, attacks

1. INTRODUCTION

The DARPA Packet Radio project which began in early 70's established the notion of ad hoc wireless networking. DARPA had a project known as packet radio, where several wireless terminals could communicate with one another on a battlefield. The word "ad hoc" entails that this network is customary for a special, often uttered on the spur of the moment service adapted to applications [1]. Ad hoc networks are of the interest owing to the lesser price of realization and the likelihood for mobility. The capability to swiftly set out them under both usual and unkind provisions has made it paramount in such environments.

An ad hoc wireless network is a network of two or more devices equipped with wireless communications and networking potential. These devices are able to commune with a further node that is instantly contained by their radio range or one that is out to their radio range. For the latter situation, an intermediate device is in role to pass on the packet from the source headed towards destination. Such devices can take diverse forms like palmtop, laptop, mobile phone etc. The computation methodology, storage and communication capabilities of these devices will vary immensely. Ad hoc devices are not only capable of to discover the existence of connectivity with neighboring devices, but can also recognize the type of the device and their corresponding characteristics.

It is worth to mention that ad-hoc networks are not an alternative or substitution of the networks with infrastructures. Their extent is in the locale where cost, environment, or application constraints require self-organized and infrastructure-less solutions [2]. Moreover the perception that a wireless ad hoc network is equivalent to a conventional tethered network except that the cables are replaced with antennas is a common misconception. Wireless ad hoc networks have unique characteristics that necessitate special solutions.

These networks are built, used, and sustained by their constituent wireless nodes over a certain geographical area. Nodes in ad hoc networks do not have a priori awareness of the topology of network. They ought to ascertain it. A node will discover its local topology by broadcasting its existence, and listening to broadcast announcements from its neighbors. With the passage of time, each node acquires to know about all other nodes and finds the ways to reach them.

An ad hoc network may be connected through dedicated gateways, or nodes functioning as gateways, to other fixed networks or the Internet. So, through this it can expand the access to fixed network services. These nodes generally have a limited transmission range and, so, each node seeks the assistance of its neighboring nodes in forwarding packets, in the case of multi hop ad hoc networks. In order to establish routes between nodes which are farther than a single hop, specially configured routing protocols are engaged. The nodes in an ad hoc network function both as a host and router, with the control of the network distributed among the nodes. The unique feature of these protocols is their ability to trace routes in spite of a dynamic topology.

The paper endows with the background knowledge to new researchers interested in pursuing research in the area of ad hoc networks. The contribution of this paper is to provide the comprehensive appraisal of ad hoc network on the basis of an exhaustive review of various related papers presented and published in reputed conference proceedings, papers published in renowned journals and even some books.

2. REVIEW OF LITERATURE

2.1 Characteristics of Ad hoc Networks

The characteristics of ad hoc networks are summarized [3][4][5] as follows

- *Infrastructure-less or with minimum infrastructure support*: An ad-hoc network is a group of mobile devices with a radio transmitter and receiver, coupled in short of or with a bare support of any fixed infrastructure.
- *Self-organizing and self-managing*: All interactions have to be executable in that absence of any third party support. The organization and management of mobile ad-hoc network is distributed along with the participating nodes.
- *Dynamic Network topology*: Nodes in ad hoc networks are open to move randomly. The network topology may change indiscriminately and have no constraint on their distance from the rest of the

nodes. Consequently, the entire topology is changing in an unpredictable way.

- *Wireless:* This type of network is wireless in nature. This characteristic of the network make it more practical but also cause complexities.
- *Node is both a host and a router*: In a mobile ad-hoc network, a packet can travel from a source to a destination either directly, or through some set of intermediate packet forwarding nodes. Therefore, nodes rely on each other to established communication, thus each node as well acts as a router.
- *Multi-hop*: The nodes in this type of network have limited range. When a source node and destination node for a message is out of the radio range, it is accomplished with multi-hop routing. Because of this support communications beyond Line of Sight (LOS) is possible at high frequencies.
- *Power constraint*: In most of the scenarios, mobile ad-hoc networks operate on low power devices. The battery exhausts because of added work executed by the node so as to survive in the network.
- *Low Transmission Range*: Such networks have a very limited transmission range because of the devices use radio or infrared frequencies for their communications. But this transmission range can be increased by using multi hop routing paths.
- *Low transmission Power*: There is gain in transmission power as it is required more for sending a signal over any distance in one long hop than in multiple shorter hops.
- *Variation in scale*: As the nodes are mobile in nature, so there is frequent addition or deletion of nodes in a network and hence there is variation in scale. Thus we can say that such networks have dynamic infrastructures.
- *Distributed*: For the central control of the network operations, the control and management of the network is distributed among the terminals
- *Heterogeneity*: The participating nodes in single network may range from mobile devices, PDAs to laptops so there is heterogeneity among the nodes.
- *Mobility* is not, however, a requirement for nodes in ad hoc networks, in ad hoc networks there may exist static and wired nodes, which may make use of services offered by fixed infrastructure
- *Economical*: They are economical in some cases, as they eliminate fixed infrastructure costs and reduce power consumption at mobile nodes. Moreover because of short communication links, radio emission levels can be kept low. This reduces interference levels, increase spectrum reuse efficiency, and makes it possible to use unlicensed unregulated frequency bands.
- *Robust*: They can be more robust than conventional wireless networks because of their non-hierarchical distributed control and management mechanisms.
- *Temporary:* Ad hoc networks are temporary networks because they are formed to fulfill a special purpose and cease to exist after fulfilling this purpose

2.2 Vulnerabilities of Ad hoc Networks

Vulnerability is any hardware, firmware, or software flaw that can cause an information system open for potential exploitation. Among the intrinsic vulnerabilities of ad hoc networks, some reside in their routing, others in their use of wireless links and still some others in their auto-configuration mechanisms. The various vulnerabilities that subsist in the mobile ad hoc networks are [6] [7] [8].

- *Channel Vulnerability*: The use of wireless links renders the network susceptible to attacks ranging from passive eavesdropping to active interfering. The attacks can come from all directions and target at any node. An attacker just needs to be within radio range of a node in order to intercept network traffic.
- *Node vulnerability*: The nodes with inadequate physical protection are receptive to being captured, compromised and hijacked.
- *Lack of infrastructure*: The lack of centralized authority means that the adversaries can exploit this vulnerability for new types of attacks designed to break the cooperative algorithms used in ad hoc networks.
- *Dynamically varying network topology* puts security of routing protocols under threat.
- *Power and computational restrictions* prevent the use of complex encryption algorithms.
- The *self organization and management* mechanism also brings up new vulnerabilities. For example, in the case of duplicate address detection (DAD), a danger exists that a malicious node may pretend to be using any of the addresses chosen by an incoming host, thus denying the incoming host the right to join the network. As a result, a node cannot make any assumption about the trustworthiness of its peers, which assist the node with its communication and, in general, does not possess their credentials

2.3 The Challenges

The ad hoc network is insecure attributable to its nature of structure. The absence of centralized machinery may reason several intricacies when there is a need to have a centralized coordinator; restricted power supply can also source some selfish problems [6]. Thus, an ad hoc network will necessitate more vigorous security design to make certain the security of it, in comparison to the wired network. An ad hoc network environment has to overcome certain issues of limitations and inefficiency [2][8][9] summarized as follows. It includes

- *Limited range of wireless transmission* – The restricted radio band consequent in less data rates as evaluated to their counterpart, wireless networks. So best possible usage of bandwidth is

obligatory by keeping minimal overhead as achievable.

- *Dynamic Nature of Topology*- The dynamic nature of network topology results in recurrent path breaks and routes often change due to mobility. Robustness of ad hoc networks in highly dynamic environments with changing load and variable speeds of the nodes is hard to achieve. Therefore, any security solution with a static configuration would not be adequate for it.
- *Recurrent network partitions*- The indiscriminate movement of nodes frequently leads to partition of the network. This typically have an effect on the intermediate nodes. The continuously changing scale of the network has set higher requirement to the scalability of the protocols and services in the mobile ad hoc network
- *Lack of defense boundaries*: As the nodes have freedom to join, leave and move inside the network, so there is no clear line of defense. The edges that divides the inside network from the outside world becomes fuzzy. This may cause some of the nodes may be compromised by the adversary and thus perform some malicious behaviors that are hard to detect;
- *Physical threats*: The portable devices and the system security information stored in it are susceptible to compromises or physical capture, particularly low-end devices with weak protection.
- *Trust on Co-operation*: The decentralized decision making in the MANET relies on the cooperative participation of all nodes. The malicious node could simply block or modify the traffic traversing it by refusing cooperation to break the cooperative algorithms.

2.4 Application Areas

There are many areas where ad hoc networks have applications [7] [10] [11] such as

- *Military tactical operations*: In hostile or unfamiliar situations establishment of military communications can be instituted in a quick manner. The vast majority of these nodes move around at varying speeds and nodes may lose connectivity to other nodes as they move around in the battlefield because of the terrain, distance among the nodes, all these issues can also be addressed by ad hoc networks.
- *Search and rescue missions*: This can be used for search and rescue operations as communication for these may have little or no wireless infrastructure support.
- *Disaster relief operations*: During major emergencies and disasters such as hurricanes or large explosions, the communications infrastructure in the immediate area of the disaster or emergency may be unusable, unavailable, or completely destroyed. Such networks are well suited for such an application because of their ability to create connectivity rapidly with limited human effort
- *Commercial use*: This type of network can be used for enabling communications in exhibitions, conferences, lectures and large gatherings.
- *Industrial use*: The other generally considered application for adhoc networks is interconnection of sensors in industrial settings. Sensors are typically small devices measuring environmental inputs such as temperature, motion, light, etc. and often alerting users and/or taking specific reactions (e.g. starting an air-conditioner) when those inputs reach specific ranges.
- More recently researchers have regarded the use of ad hoc networks in the *vehicular environment.* Allowing ad hoc networking capabilities accessible in such environments can facilitate a variety of new applications such as sharing of up-to-date traffic information among vehicles.

2.5 Routing in Ad hoc Networks

In multi-hop networks, source and destination nodes can be away from each other by multiple hops, and therefore packets may require to be forwarded by multiple nodes on the path from source to destination. This forwarding progression of packets is known as routing. The flow of data to one destination is called uni-cast routing. On the other hand, for multiple destinations, this flow of data is multicast routing and if all the nodes in the network are destined by the source, then these types of flows are known as broadcast routing.

An exclusive mixture of characteristics of ad hoc networks composes routing in it remarkable. First, a highly dynamic network with frequent topological changes, because of the nodes in this network is permissible to move in an unrestrained mode, cause frequent route failures. A good routing protocol for this network environment has to dynamically adapt to the changing network topology. Second, the underlying wireless channel provides much lower and more variable bandwidth than wired networks. The wireless channel working as a shared medium takes available bandwidth per node even lower. So routing protocols should be bandwidth efficient by expending a minimal overhead for computing routes so that much of the remaining bandwidth is available for the actual data communication. Third, nodes run on batteries which have limited energy supply. In order for nodes to stay and communicate for longer periods, it is desirable that a routing protocol be energy efficient as well [4]. Thus, routing protocols must meet the conflicting goals of dynamic adaptation and low overhead to deliver good overall performance. The widely accepted classification of routing protocols for ad hoc networks is as follows [12]

2.5.1 Re-active routing protocols

- These type of protocols do not take initiatives for finding routes
- The routes are established “on demand” by flooding a query regarding it.

Pros and cons:

- They do not used use bandwidth except when needed to find a route
- The flooding process of querying for routes causes much network traffic
- There is initial delay in traffic

2.5.2 Pro-active routing protocols

Every proactive routing protocol usually needs to maintain accurate information in their routing tables. It attempts to continuously evaluate all of the routes within a network. When a packet needs to be forwarded, a route is already known and can be used immediately.

- The routes are set up based on continuous control traffic
- All routes are maintained all the time

Pros and cons:

- There is constant overhead created by control traffic
- The routes are always available
- Respective amount of data for maintaining routing information
- Slow reaction on restructuring network and failure of individual nodes.

2.5.3 Hybrid Protocols

- They combine merits of both reactive and pro active protocols
- Normally they exploit network hierarchical structure.

2.6 Authentication in Ad hoc Networks

Authentication is a phase of communication network security procedure to ensure that the principals with whom one interacts are the expected ones. Granting resources to, obeying an order from, or sending confidential information to a principal of whose identity we are unsure is not the best strategy for protecting availability, integrity and confidentiality [13]. Authentication [14] is a process that involves an authenticator communicating with a supplicant using an authentication protocol to verify credentials presented by the supplicant in order to determine the supplicant's access privileges. A Trusted Third Party (TTP) may be involved as part of the authentication protocol.

The supplicant is an individual or an entity that is with the purpose of to have access to any protected resources is being authenticated through an authenticator. An authenticator is an entity that is meant for protecting and controlling access to some resources. The authenticator carries out the course of authentication and makes decisions of authentication. An authentication protocol is a sequence of message exchanges between supplicant(s) and authenticator(s) that either distributes secrets to some of those principals or allows the use of some secret to be recognized. A supplicant is authenticated by an identifier known as credential. Lastly, a Trusted Third Party is an entity that is commonly having faith by the supplicant and the authenticator and that can accomplish mutual authentication between the two parties. The provisions of entity authentication and authenticated key establishment among nodes are together target intents in securing of ad hoc networks [15]. Some of the examples of authentication protocols are ARAN (Authenticated Routing for Ad hoc Networks), Ariadane, LHAP (Lightweight Hop-by-hop Authentication Protocol) and SAR (Security-aware Ad hoc Routing).

Classification of authentication Protocols

An authentication protocol is classified as per the following classification [13]

- *Homogeneous vs Heterogeneous*: based on the roles assigned to nodes in the network with respect to the authentication operation.
- *Possession vs Context*: identifies the supplicant based on a unique possession, while the second class identifies the supplicant based on context
- *Prior vs Post node deployment*: Some protocols establish credentials prior to node deployment, while other protocols assume credentials are established post node deployment.

2.7 Attacks on Adhoc Networks

An attack is an effort to evade the security controls on a computer. The attack may target to alter, release, or deny data. Attacks not in favor of the network may come from malicious nodes that are not may be the component of the network and are attempting to join the network illegitimately. The success of an attack depends on the vulnerability of the system and the efficacies of existing countermeasures. There are number of attacks that are designed to exploit the vulnerabilities of ad hoc networks

There are two types of security attacks [7][16]:

- passive
- active

- In a ***passive attack,*** a malicious node either ignores operations supposed to be accomplished by it or listens to the channel, attempting to retrieve valuable information. However, this process of gathering information might lead to active attacks later on.
- In an ***active attack,*** information is inserted to the network and thus the network operation or some nodes may be harmed.

A number of attacks have been identified for the ad hoc networks. Some of the common known attacks found in literature are as follows [8][17][18].

Wormhole Attack

A particularly severe security attack, called the wormhole attack, has been introduced in the context of ad-hoc networks. During the attack a malicious node captures packets from one location in the network, and tunnels them to another malicious node at a distant point, which replays them locally [19]. A very simple end-to-end algorithm to handle wormhole attacks on ad hoc networks with variable communication ranges was presented. [20]

Black Hole Attack

Black hole attack is one of these. In this type of attack, a malicious node which absorbs and drops all data packets makes use of the vulnerabilities of the on demand route discovery protocols, such as AODV. Black hole behavior may also be due to a damaged node dropping packets unintentionally. In any case, the end result of the presence of a black hole in the network is lost packets. [21]. A paper proposes a collaborative architecture to detect and exclude malicious nodes that act in groups or alone. [22]

Flooding Attack

The data flooding attack sends many data packets in order to clog not only a victim node but also the entire network since all packets are transmitted via multiple hops. Hence, data flooding attacks are extremely hazardous to wireless ad hoc networks. [23]

Jamming Attack

A particular class of DoS attacks called Jamming. In fact, the mobile hosts in mobile ad hoc networks share a wireless medium. Thus, a radio signal can be jammed or interfered, which causes the message to be corrupted or lost. If the attacker has a powerful transmitter, a signal can be generated that will be strong enough to overwhelm the targeted signals and disrupt communications. There are many different attack strategies that a jammer can perform in order to interfere with other wireless communications. [24]

Denial of Services Attack

The DoS attack results when the network bandwidth is hijacked by a malicious node [25]. The attacker injects packets into the network in an attempt to consume valuable network resources such as bandwidth, or to consume node resources such as memory or computation power. So the routing tables overflow attack and energy consumption attack can be regarded as the specific instances of DoS attack.

Byzantine Attack

Byzantine attack It is also been called impersonation attack, in which a malicious node may impersonate another normal node and send false routing information to create an anomaly update in the routing table. Furthermore, an attacker might gain unauthorized access to resource and sensitive information. [26]

Link Withholding Attack

In this attack, a malicious node ignores the requirement to advertise the link of specific nodes or a group of nodes, which can result in link loss to these nodes **[18]**.

Link Spoofing Attack

In a link spoofing attack, a malicious node advertises fake links with non-neighbors to disrupt routing operations **[18].**

Colluding Mis-Relay Attack

In this attack, multiple attackers work in collusion to modify or drop routing packets to disrupt routing operation in an ad hoc network **[**18].

Replay Attack

In a replay attack [27], a node records another node's valid control messages and resends them later. This causes other nodes to record their routing table with stale routes. Replay attack can be misused to impersonate a specific node or simply to disturb the routing operation.

Rushing attack

This is a malicious attack that is targeted against on-demand routing protocols that use duplicate suppression at each node. An attacker disseminates ROUTE REQUESTS quickly throughout the network, suppressing any later legitimate ROUTE REQUESTS when nodes drop them due to the duplicate suppression [28].

In addition to the above listed following are the some attacks are also quoted in the literature [17] [29].

- *Malign***:** Watchdog and path-rater are used in ad hoc routing protocols to keep track of perceived malicious nodes in a blacklist. An attacker may blackmail a good node, causing other good nodes to add that node to their blacklists, thus avoiding that node in routes.
- *Partition*: An attacker may try to partition the network by injecting forged routing packets to prevent one set of nodes from reaching another.
- *Detour***:** An attacker may attempt to cause a node to use detours through suboptimal routes. Also compromised nodes my try to work together to create a routing loop.
- *Routing table poisoning***:** The publication and advertisement of fictitious routes.
- *Packet replication***:** The replication of stale packets, to consume additional resources such as bandwidth, etc.
- *Bad Mouthing Attack*: The malicious parties can provide dishonest recommendations to frame up good parties and/or boost trust values of malicious peers.
- *On-off Attack***:** malicious entities behave well and badly alternatively, hoping that they can remain undetected while causing damage.
- *Sybil*: Assuming the identity of several nodes in the network.
- *Traffic Snooping***:** A form of eavesdropping where the attacker reads exposed information to gain insight into a node or network's behavior
- *Fabrication:* an unauthorized party not only gains the access but also inserts counterfeit objects into the system
- *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.
- *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.
- *Newcomer attack*: A malicious node may remove their bad reputation/distrust by registering as a new user.
- *Incomplete information*: A malicious node may not cooperate in providing proper or complete information. Usually compromised nodes collude to perform this attack.
- *False information or false recommendation*: A malicious node may collude and provide false recommendations/information to isolate good nodes while keeping more malicious nodes. This attack also called a black-mounting attack.

- *Spoofing* is occurred when a malicious node misrepresents its identity in the network and alters the target of the network topology that a benign node can gather.
- *Gray-hole attack*: A malicious node may selectively drop packets, as a special case of black hole attack.
- *Selective misbehaving attack*: A malicious node may selectively provide or deny proper services.

The Table 1 shows the layer target by some of these attacks

Table 1: Attacks on Protocol Stack [30]

Layer	Attacks
Application Layer	Repudiation, data corruption
Transport Layer	Session hijacking, SYN flooding
Network Layer	Wormhole, Black Hole, Byzatine, Flooding, Resource Consumption, Location disclosure
Data Link Layer	Traffic analysis, monitoring
Physical Layer	Jamming, Eavesdropping
Multi Layer attacks	Replay, Impersonation, DoS, man in the middle

3. CONCLUSION

A number of solutions are proposed which lessen the vulnerability of ad-hoc networks to some extent. One single security solutions can not protect against all kinds of different attacks against a mobile ad hoc network. Thus, a goal for ad hoc networks is to apply a multi-defense security solution that offers multiple lines of defense against many different attacks. The solution relies on multiple defenses, spanning different devices and different layers in the protocol stack.

Due to the miscellany in such communication system and the rise in requirement of cooperation among diverse nodes, other sorts of security risks are pioneered. A node, even after getting through the traditional cryptographic hard security tests (authorization and access) can get advantage by reporting false measurement results. These security risks are reported as ‘‘soft security threats’’ as they deal with main beliefs like honesty and reliability.

4. REFERENCES

[1] Mario Gerla, “Adhoc networks: Emerging Applications, Design Challenges and Future Opportunities” *Prasant Mohapatra and Srikanth V. Krishnamurthy,(eds), Adhoc Networks: Technologies and Protocols*, Springer Verlag, pp. 1-22, 2005

[2] Andr´e Weimerskirch and Gilles Thonet, “A Distributed Light-Weight Authentication Model for Ad-hoc Networks,” in *Proc. of International Conference on Information Security and Cryptology (ICISC 2001)*, pp. 341-354, December 2001

[3] Hekmat Ramin, Ad hoc Networks: Fundamental Properties and Network Topologies. Springer , 2006

[4] Mahesh K. Marina and Samir R. Das , “ Routing in Mobile Adhoc Networks,” P. Mohapatra and S. V. Krishnamurthy(eds), Ad Hoc Networks: Technologies and Protocols , *Springer*, Sep 2004.

[5] A. Naveed and S. S. Kanhere, “Authentication and Privacy in Wireless Ad-hoc Networks”, R. Beyah, J. McNair and C. Corbett (eds.), *Security in Ad-hoc and Sensor Networks*, World Scientific Press, July 2009

[6] Li Wenjia and Joshi Anupam ,” Security Issues in Mobile Ad hoc networks -A Survey,” *The 17th White House Papers Graduate Research In Informatics at Sussex*, pp.1-23, 2004.

[7] Farooq Anjum and Petros Mouchtaris, *Security for Wirelss Ad hoc Networks*. Wiley-InterScience, A John Wiley & Sons Inc., Publication, 2007

[8] Mishra Amitabh and NadKarni Ketan M., “Security in Wireless Adhoc Networks,” *Mohammad Ilyas (ed.), The Handbook of Adhoc Wireless Networks, Chapter 30*, CRC Press, 2003

[9] Yang Hao, Luo Haiyun, Ye Fan, Lu Songwo and Zhang Lixio, “Security in Mobile Ad Hoc Networks: Challenges and Solutions,” *IEEE Wireless Communications*, vol. 11, issue 1, pp. 38-47, Feb 2004

[10] Michele Nogueira Lima, Aldri Luiz dos Santos, and Guy Pujolle, “A Survey of Survivability in Mobile Ad Hoc Networks,” *IEEE Communications Surveys & Tutorials*, vol. 11, no. 1, pp. 66-77, 2009.

[11] Tavli, Bulent and Heinzelman, Mobile Adhoc networks. Wendi 2006,

[12] Changling Liu and Jorg Kaiser, “A Survey of Mobile Ad Hoc Network Routing Protocols,” TR-4, MINEMA, University of Magdeburg, October 2005

[13] Nidal Aboudagga, Mohamed Tamer Refaei, Mohamed Eltoweissy, Luiz A. DaSilva, and Jean-Jacques Quisquat, “Authentication Protocols for Ad Hoc Networks: Taxonomy and Research Issues,” in *Proc. of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks*, pp. 96-104, 2005

[14] A.O. Salako “Authentication in Ad hoc Networking,” in *Proc. of London Communications Symposium 2002, 2002*

[15] K. Hoeper and G. Gong, *“*Pre-Authentication and Authentication Models in Ad Hoc Networks,*” Y. Xiao, X. (Sherman) Shen, and D.-Z. Du (eds.), Wireless/Mobile Network Security, Springer-Verlag*, 2006

[16] Bing Wu, Jianmin Chen, Jie Wu and Mihaela Cardei, “A Survey on Attacks and Countermeasures in Mobile Adhoc Networks,” *Xiao, X. Shen, and D.-Z. Du (Eds.), Wireless/Mobile Network Security, Springer, Chapter 12*, pp. 103-135, 2006

[17] Loay Abusalah, Ashfaq Khokhar, and Mohsen Guizani, “A Survey of Secure Mobile Ad Hoc Routing Protocols,” *IEEE Communications Surveys & Tutorials*, vol. 10, no. 4, pp. 78-93, 2008

[18] Bounpadith Kannhavong, Hidehisa Nakayama, Yoshiaki Nemoto, and Nei Kato, “A Survey Of Routing Attacks In Mobile Ad Hoc Networks,” IEEE Wireless

Communications, vol. 14, issue 5, pp. 85-91, October 2007

[19] Marianne A.Azer, Sherif M. El-Kassas and Magdy S. El-Soudani, "A Full Image of the Wormhole Attacks Towards Introducing Complex Wormhole Attacks in Wireless Ad Hoc Networks," *International Journal of Computer Science and Information Security*, vol.1, no. 1, pp. 41-52, May 2009

[20] Khurana S. and Gupta N, "FEEPVR: First End-to-End protocol to Secure Ad hoc Networks with variable ranges against Wormhole Attacks," in *Proc. Of IEEE International Conference on Emerging Security Information, Systems and Technologies*, pp 74-79, 2008

[21] Dokurer S., Ert, Y.M and Acar C.E.," Performance analysis of ad-hoc networks under black hole attacks," in *Proceedings of IEEE SoutheastCon*, pp. 148-153, 2007

[22] Patcha A and Mishra A, "Collaborative Security Architecture for Black Hole Attack Prevention in Mobile Ad Hoc Networks," in *Proc. of IEEE conference on Radio and Wireless*, pp. 75-78, 2003

[23] Hyojin Kim, Ramachandra Bhargav Chitti, and JooSeok Song, "Novel Defense Mechanism against Data Flooding Attacks in Wireless Ad Hoc Networks," *IEEE Transactions on Consumer Electronics*, vol. 56, issue 2, pp. 579-582,May 2010

[24] Ali Hamieh and Jalel Ben-Othman, "Detection of Jamming Attacks in Wireless Ad Hoc Networks using Error Distribution," in *Proc. of IEEE Conference on Communications*, pp. 1-6, 2009

[25] N. Uushona and W T Penzhorn, "Towards the Security of Routing in Ad Hoc Networks," *IEEE International Symposium on Industrial Electronics*, pp. 1783-1788, June 2005.

[26] Ming Yu, Kulkarni S. and Lau, P, "A New Secure Routing Protocol To Defend Byzantine Attacks For Ad Hoc Networks, "in *Proc. of 13th IEEE International Conference on Networks*, pp. 6, Nov 2005

[27] C. Adjih, D. Raffo, and P. Muhlethaler, "Attacks Against OLSR: Distributed Key Management for Security," in *Proc. 2nd OLSR Interop/Wksp*., July 2005.

[28] Yih-Chun Hu.and Perrig A.,"A Survey of Secure Wireless ad hoc routing," *IEEE Security and Privacy*, vol. 2, issue 3, pp. 28-39, 2004

[29] Esch J., "Prolog to A Survey of Trust and Reputation Management Systems in Wireless Communications," *Proceedings of the IEEE*, vol. 98, issue 10, October 2010.

[30] Bing Wu, Jianmin Chen, Jie Wu and Mihaela Cardei, "A Survey on Attacks and Countermeasures in Mobile Adhoc Networks," *Xiao, X. Shen, and D.-Z. Du (Eds.), Wireless/Mobile Network Security, Springer, Chapter 12*, pp. 103-135, 2006