Improvement authentication of routing protocols for Mobile Ad Hoc networks

Ahmad Alomari
Bucharest University
Dept. of Mathematics and Informatics
alomari.jordan@gmail.com

Abstract - **Ad Hoc network Consist of mobile hosts (or nodes) which communicate with other nodes through wireless medium without any fixed infrastructure . Dynamic network topology : the mobile nodes are free to move randomly and organize themselves arbitrarily the wireless links in this network are highly error prone and can do down frequently due to mobility of nodes , interference and less infrastructure . therefore , routing in MANET is a critical task due to highly dynamic environment In recent years , several routing protocols have been proposed for mobile ad hoc networks ; to increase the secure path between the nodes . I focus on my scheme on authentication between the nodes and I choose Ad Hoc On-Demand Distance Vector (AODV) protocol to apply this scheme , which it depend on hash function , hash lock and random number generation , this scheme use to produce secure and authentication environment between the nodes In Mobile Ad Hoc Network.**

Keywords —**authentification, routing protocol, hash function, AODV, metaID.**

I . INTRODUCTION

A mobile ad hoc net work (MANET) is a system wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topology . People and vehicles can thus be internet worked in areas without preexisting communication infrastructure or when the use of such infrastructure requires wireless extension. In the mobile ad hoc network node can directly communicate with all other nodes within their radio ranges, where as nodes that not in the direct communication range use intermediate node to communicate with each other. In this two situation all the nodes that have participated in the communication automatically form a wireless network , therefore this kind of wireless network can be viewed as mobile ad hoc network The trust relationships established between network nodes could be used for the provision of higher level security solutions, such as key management. In[2], and [3], threshold cryptography has been proposed to provide a reliable, distributive key management for MANET by exploiting some nodes as a trust anchor for the rest of the network.

Some aspects of ad hoc networks have interesting security problem, routing is one such aspect ,several routing protocols for ad hoc networks have been developed to produce a secure environment between the nodes In ad hoc networks ,In my scheme I can apply this In the most kinds of the routing protocol ,and I choose the AD ho on-demand Distance Vector (AODV) cause It Is the most popular between the routing protocols and they use widely[4] ; I focus In this paper on the authentication between the nodes , to sure that the networks accessible by authorize nodes.

In this paper first section I make short interview for the related and previous works in improvement of ad hoc on-demand distance vector (AODV).

In section 2 talk about security goals and challenges on routing protocols of MANETs , this goals like availability and authorization ,and the challenges like dynamic topology and security , and this the main challenges in mobile ad hoc networks (MANETs) cause this kind of network does not rely on any fixed infrastructure and centralize control. Section 3 talk about the most attacks on MANETs (like impersonate) and routing protocols like rushing attack and routing table overflow, section 4 speak in general about ad hoc on-demand distance vector protocol (AODV) and make short view and how it start work, section 5 speak about my scheme the idea of this scheme is used the hash function and use hash lock to increase the authentication between the nodes when they start communicating in the ad hoc network.

II . RELATED WORK

There are many works that improve the security routing protocols especially in On Demand routing protocols. Denh Sy, Rex Chen and Lichun Bao [5] proposed On-Demand Anonymous Routing in Ad Hoc Networks ODAR, an On-Demand Anonymous Routing protocol, which provides node, link and path anonymities in ad hoc networks based on Bloom filters.

The use of Bloom filters additionally gives ODAR the storage-, processing- and communication-efficiencies, making it suitable in the ad hoc network environments.
Castelluccia et al. were the first to use Bloom filters to compress source route information after the source route is discovered using DSR [6], [7]. However, no research was found so far that uses Bloom filters for anonymous source routing purposes.

Dahill et al. [8] proposed ARAN, a routing protocol for ad hoc networks that uses authentication and requires the use of a trusted certificate server. In ARAN, every node that forwards a route discovery or a route reply message must also sign it, (which is very computing power consuming and causes the size of the routing messages to increase at each hop), whereas the proposal presented here only require originators to sign the message.

SAODV [9]. The Secure Ad hoc On-Demand Distance Vector protocol was proposed to answer the challenge of securing a MANET network. SAODV is an extension of the AODV routing protocol, and it can be used to protect the route discovery mechanism by providing security features like integrity, authentication and non-repudiation. SAODV assumes that each ad hoc node has a signature key pair from a suitable asymmetric cryptosystem. Further, each ad hoc node is capable of securely verifying the association between the address of a given ad hoc node and the public key of that node.

In SEAD [10] (by Hu, Johnson and Perrig) hash chains are also used in combination with DSDV-SQ [3] (this time to authenticate hop counts and sequence numbers). At every given time each node has its own has chain. The hash chain is divided into segments; elements in a segment are used to secure hop counts in a similar way as it is done in SAODV. The size of the hash chain is determined when it is generated.

Papadimitratos and Haas [11] proposed a protocol (SRP) that can be applied to several existing routing protocols (in particular DSR [9] and IERP [10]). SRP requires that, for every route discovery, source and destination must have a security association between them. Furthermore, the paper does not even mention route error messages. Therefore, they are not protected, and any malicious node can just forge error messages with other nodes as source.

Ariadne [12], by the same authors, is based on DSR [9] and TESLA [11] (on which it is based its authentication mechanism). It also requires clock synchronization, which is, arguably, an unrealistic requirement for ad hoc networks. Every member of the team would know the key and, therefore, it would be able to encrypt and decrypt every single packet. Nevertheless, this does not scale well and the members of the team have to trust each other. So it can be only used for a very small subset of the possible scenarios.

III. SECURITY GOALS AND CHALLENGES IN ROUTING PROTOCOL OF MANET

The preliminary security goals can be considered as an extension of the objectives for traditional networks.
In providing a secure networking environment some or all of the following service may be required , in other words, what should be covered in the security criteria for the mobile ad hoc network when we want to inspect the security state of the mobile ad hoc network [13]. In the following, I briefly introduce the widely-used criteria to evaluate if the mobile ad hoc network is secure.

A. Security goals of routing protocol of MANET:

- Availability

Availability ensures the survivability of network services despite denial of service attacks. A denial of service attack could be launched at any layer of an ad hoc network.. On the network layer, an adversary could disrupt the routing protocol and disconnect the network. On the higher layers, an adversary could bring down high-level services. One such target is the key management service, an essential service for any security framework.

- Confidentiality

Confidentiality means that certain information is only accessible to those who have been authorized to access it. In other words, in order to maintain the confidentiality of some confidential information, we need to keep them secret from all entities that do not have the privilege to access them.

- Integrity

Integrity guarantees that a message being transferred is never corrupted. A message could be corrupted because of benign failures, such as radio propagation impairment, or because of malicious attacks on the network.

- Nonrepudiation

Nonrepudation ensures that the origin of a message cannot deny having sent the message. Nonrepudiation is useful for detection and isolation of compromised nodes. When a node A receives an erroneous message from a node B, non-repudiation allows A to accuse B using this message and to convince other nodes that B is compromised.

- Authorization

Authorization is a process in which an entity is issued a credential, which specifies the privileges and permissions it has and cannot be falsified, by the certificate authority. there should be an authorization process before the network administrator accesses the network management functions [14].

B. Challenges in mobile ad hoc network

In a mobile ad hoc network, all the nodes cooperate with each other to forward the packets in the network, and hence each node is effectively a router. Thus one of the most important issues is routing. Now I describe some of issues in ad hoc network:

- Distributed network**:** A MANET is a distributed wireless network without any fixed infrastructure That means no centralized server is required to maintain the state of the clients.
- Dynamic topology: The nodes are mobile and hence the network is self- organizing. Because of this, the topology of the network keeps changing over time. Consequently, the routing protocols designed for such networks must also be adaptive to the topology changes.
- Power awareness: Since the nodes in an ad hoc network typically run on batteries and are deployed in hostile terrains. This implies that the underlying protocols must be designed to conserve battery life.
- Addressing scheme: The network topology keeps changing dynamically and hence the addressing scheme used is quite significant.. In wireless

WAN environments, Mobile IP [15] is being used. Because the static home agents and foreign agents are needed, hence, this solution is not suitable for ad hoc network.

- Network size: The ability to enable commercial applications such as voice transmission in conference halls, meetings, etc., is an attractive feature of ad hoc networks. However, the delay involved in the underlying protocols places a strict upper bound on the size of the network.
- Security: many new threats are emerging on ad hoc networks and they are hard to defend with the conventional security schemes, popular in their wired equivalent. Mobility and limited range of transmission makes it difficult to detect any malicious activity in ad hoc networks. Network layer is most susceptible to the attacks because of inherent peer-to peer communication model. A malicious node can voluntarily become a router and disrupt the normal network operations. A mobile node without adequate protection can be easy impersonate. A malicious node might over hear the channel and modify the flow or traffic.

IV SUMMARY OF THE MOST ATTACKS IN MANETAND ROUTING PROTOCOL

In general, the attacks on routing protocols can generally be classified as routing disruption attacks [18][17] and resource consumption attacks [16][18]. In routing disruption attacks, the attacker tries to disrupt the routing mechanism by routing packets in wrong paths; in resource consumption attacks, some non-cooperative or selfish nodes may try to inject false packets in order to consume network bandwidth. I depicts a broader classification of the possible attacks in MANETs

A. Impersonation

Impersonation attack is a severe threat to the security of mobile ad hoc network [4]. As we can see, if there is not such a proper authentication mechanism among the nodes, the adversary can capture some nodes in the network and make them look like benign nodes. In this way, the compromised nodes can join the network as the normal nodes and begin to conduct the malicious behaviors such as propagate fake routing information and gain inappropriate priority to access some confidential information.

B. Modification

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

C. Flooding attack

In flooding attack, attacker exhausts the network resources, such as bandwidth and to consume a node's resources, such as computational and battery power or to disrupt the routing operation to cause severe degradation in network performance. For example, in AODV protocol, a malicious node can send a large number of RREQs in a short period to a destination node that does not exist in the network.

D. Black hole attack

In a black hole attack, a malicious node sends fake routing information, claiming that it has an optimum route and causes other good nodes to route data packets through the malicious one. For example, in AODV, the attacker can send a fake RREP to the source node, claiming that it has a sufficiently fresh route to the destination node.. Therefore, all traffic will be routed through the attacker, and therefore, the attacker can misuse or discard the traffic.

E. Wormhole attack

A wormhole attack [13] is one of the most sophisticated and severe attacks in MANETs. In this attack, a pair of colluding attackers record packets at one location and replay them at another location using a private high speed network. to find secure routes, that is, routes that do not include the adversary node. It is extremely difficult to detect such attacks in ad hoc wireless networks.

F. Routing Attacks

There are several types of attacks mounted on the routing protocol which are aimed at disrupting the operation of the network. Various attacks on the routing protocol are described briefly below [14] [15]:

1) Routing Table Overflow: In this attack, the attacker attempts to create routes to nonexistent nodes. Proactive routing algorithms attempt to discover routing information even before it is needed, while a reactive algorithm creates a route only once it is needed. An attacker can simply send excessive route advertisements to the routers in a network. Reactive protocols, on the other hand, do not collect routing data in advance.

2) Routing Table Poisoning: Here, the compromised nodes in the networks send fictitious routing updates or modify genuine route update packets sent to other uncompromised nodes. Routing table poisoning may result in suboptimal routing, congestion in portions of the network, or even make some parts of the network inaccessible.

3) Packet Replication: In this attack, an adversary node replicates stale packets. This consumes additional bandwidth and battery power resources available to the nodes and also causes unnecessary confusion in the routing process.

4) Route Cache Poisoning: In the case of on-demand routing protocols (such as the AODV protocol [14]), each node maintains a route cache which holds information regarding routes that have become known to the node in the recent past. Similar to routing table poisoning, an adversary can also poison the route cache to achieve similar objectives.

5) Rushing Attack: On-demand routing protocols that use duplicate suppression during the route discovery process are vulnerable to this attack. Any route discovered by the source node would contain the adversary node as one of the intermediate nodes. Hence, the source node would not be able to find secure routes, that is, routes that do not include the adversary node. It is extremely difficult to detect such attacks in ad hoc wireless networks.

V. VIEW AD HOC ON DEMAND DISTANCE VECTOR AODV:

Is a reactive unicast routing protocol for mobile ad hoc network . AODV only needs to maintain the routing information about the active path [19]. This protocol can be called a pure on-demand route acquisition system ; nodes that do not lie on active paths neither maintain any routing information nor participate in any periodic routing table exchanges. Further; a node does not have to discover and maintain a route to another node until the two need to communication , unless the former node is offering its services as an intermediate forwarding station to maintain connectivity between two other nodes . When the local connectivity of the mobile node is of interest , each mobile node can become aware of the other nodes in its neighborhood by the use of several techniques, including local (not system-wide) broad casts known as hello messages . The routing tables of the nodes within the neighborhood are organized to optimize response time to local movements and provide quick response time for requests for establishment of new routes.

AND the Ad Hoc O-Demand distance Vector (AODV) has two phases. I summarize this phase as follows:

A – Route discovery

In this phase, the source node searches a route by broadcasting route request (RREQ) packets to its neighbors [19]. Each of the neighbor nodes that has received the RREQ broadcast then checks the packet to determine which of the following conditions apply: (a) Was this RREQ received before ? (b) Is the TTL (Time To Live) counter greater than zero? (c) Is it itself the destination of the RREQ? (d) Should it broadcast the RREQ to its neighbors? When the RREQ packet reaches the destination node, the destination node sends a reply packet (RREP) on the reverse path back to the sender. This RREP contains the recorded route to that destination.

Figure 1 shows an example of the route discovery phase. When node A wants to communicate with node G, it initiates a route discovery mechanism and broadcasts a request packet (RREQ) to its neighboring nodes B, C and D as shown in the figure. However, node C also receives the same broadcast packets from nodes B and D. It then drops both of them and broadcasts the previously received RREQ packet to its neighbors. The other nodes follow the same procedure. When the packet reaches node G, it inserts its own address and reverses the route in the record and unicasts it back on the reversed path to the destination which is the originator of the RREQ.

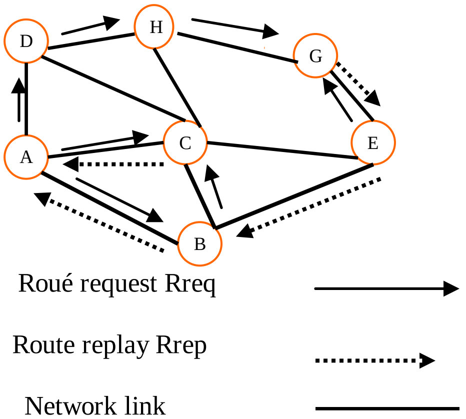

Figure 1: route discovery of AODV

B - Route Maintenance (phase 2)

The route maintenance phase is carried out whenever there is a broken link between two nodes. A broken link can be detected by a node by either passively monitoring in promiscuous mode or actively monitoring the link [21]. As shown in Figure 2. When a link break (C – H) happens, a route error packet (RERR) is sent by the intermediate node back to the originating node [21]. The source node re-initiates the route discovery procedure to find a new route to the destination. It also removes any route entries it may have in its cache to that destination node.

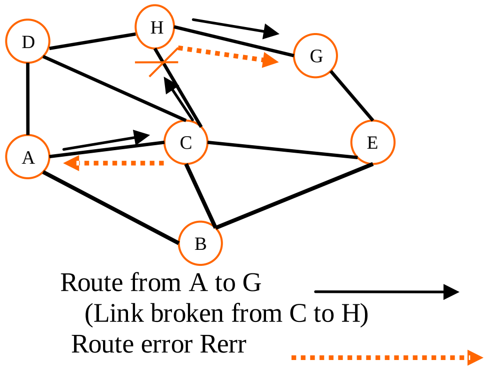

Figure 2: route maintenance of AODV

VI. AUTHENTIFICATION ON AD HOC ON-DEMAND DISTANCE VECTOR (A-AODV)

Access control mechanisms are frequently based on public key cryptographic primitive or symmetric key primitives requiring secure key distribution. And in my work the hash locks are simple access control mechanism based on one-way hash function. Every node in the hash lock scheme will be equipped with a hash function. Here even the mobile ad hoc network uses asymmetric cryptography or symmetric cryptography. This scheme is suitable for both keys used public/private key , or secret key

Now every node has the key and then computing the hash value of the key , the hash output is desired as the metaID of the node for example: node A compute the hash function for his key then the metaID for node A is H(Ka) now the node will store the metaID ,and every node store his metaID and also the all metaIDs for all nodes in the MANET (mobile ad hoc network)

If node A wants to send packet to node G , first we use this scheme to sure that node G is the authenticated node (destination node) .

We can summarize this scheme by this steps (see figure 3):

- node A sends query to the destination node (node G) this query : who are you ?
- node G sends his metaID to node A when he receives the query
- when node A receives the metaID of nod G he starts in his metaIDs storage which one has the same value
- node A sends to node G his key

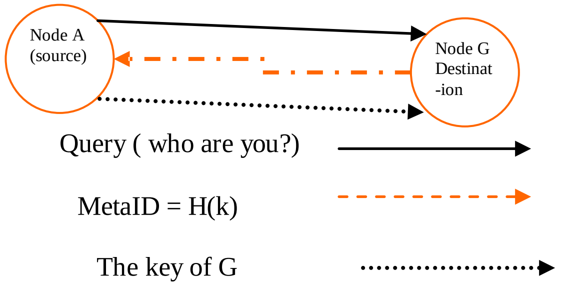

Figure 3. Hash lock scheme on AODV protocol

Here in this scheme the attacker can track the node belonging to any network and can send much queries to the node and the node will responds of this queries with the same value (as in fig 4) and cause the attacker have the same value in every respond he can tracking the key or know the hash function .

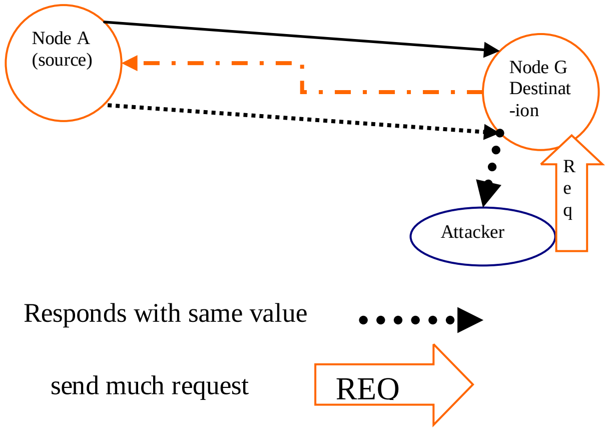

Figure 4: attack on the hash lock authentication scheme

So to improve previous scheme I use random number generation in this scheme to prevents the attackers tracking the routing protocols.

Random Hash Lock for authentication in AODV :

Every node here stores all the IDs of the nodes in the network (IDs = keys or = Fi (k)).I present a practical heuristic based one- way hash functions, I also offer a theoretically stronger based on pseudo random function (PRF) .

As in hash lock scheme the node are equipped with one-way hash function, but now also have the random number generator, now if two nodes want to communicate in the mobile ad hoc network I can apply this scheme to make authentication between them and I explain this scheme by the example:

If node A (source node) wants to communicate with the destination node like node G node A first sends a simple query to the destination node (node G), when node G receives this query it generates random number R the nonce chosen uniformly then node G hash this nonce concatenated with the BID, Finally node G sends replay to source node (node A) consisting of both the nonce and the hash output that is the pair (R, h (IDg\\ R)).

When a legitimate node (node A) receives the pair (R ,h(IDg\\R) it performs a brute-force search of all known IDs by hashing each of them concatenated with R until it finds a match; the source node (node A) now knows IDg value ; I summarize this steps also in figure 5

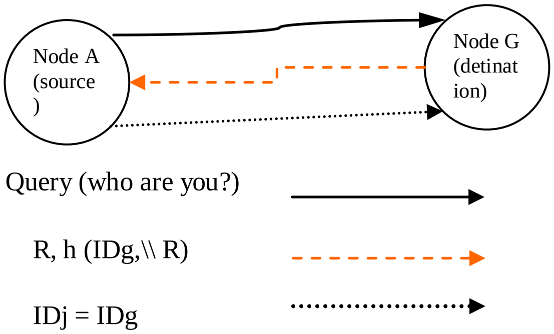

Figure 5 randomize hash lock for authentication on AODV protocol

- node A send query to node G
- node G generate a random nonce R and compute hash(IDg\\ R) .
- Node G (the destination) send (R , hash(IDg,\\R)) to node A (source)
- Node A compute hash(IDj \\ R) for all its known IDies values
- If node A find a match such that hash (IDj \\ R) = hash (IDg \\ R) , then node A send IDj to node G (destination node)
- Node G unlock itself if it receive IDj = IDg

In final when the authentication satisfy between the nodes the nodes can start send and receive the data in secure way between them by providing features like integrity ,

authentication and non- repudiation. And here the attacker is very hard to track the nodes because they change R (random number) in every routing request or routing replay .
After that the nodes in the ad hoc networks want to send or receive packet they will use hash
function and digital signature in every routing request Rreq and routing replay Rrep

Hash chain is used to check the integrity of the hop count field of RREQ and RREP messages by allowing every node that receives the message to verify that the hop count has not been modified by malicious nodes. A hash chain is formed by repeatedly applying a one-way hash function to a seed number [22]

After the hash schemes I use the digital signatures ; the digital signature is used to protect the integrity of the non-mutable data in RREQ and RREP messages.

When the node receiving a RREQ message, a node first verifies the signature before creating or updating a reverse route to the source of the RREQ. If the RREQ was received with a Double Signature Extension, then the node will also store the signature for the RREP and the lifetime (which is the 'reverse route lifetime' value) in the route entry. An intermediate node will reply to a RREQ with a RREP only if it fulfills the AODV's requirements and the node has the corresponding signature and old lifetime to put into the Signature and Old Lifetime fields of the RREP Double Signature Extension. Otherwise, it will rebroadcast the RREQ as it has no cached route. When the destination receives a RREQ, it will reply with a RREP with a Single Signature Extension. When a node receives a RREP, it first verifies the signature before creating or updating a route to that host. If the signature verification is successful, it will store the route with the signature of the RREP and the lifetime. Otherwise the RREP is discarded.

CONCLUSION

In this paper, I proposed anew scheme for authentication between the nodes in Mobile Ad Hoc Networks, it is depend on hash lock and random number generation, this scheme apply on routing protocol after discovery phase and before transfer any data or packet between the nodes , the result of this scheme the source node and destination node satisfy authentication between them when they start communicating.

REFERENCES

[1] Marco Conti, Body, Personal and Local Ad Hoc Wireless Networks, in Book The Handbook of Ad Hoc Wireless Networks (Chapter 1), CRC Press LLC, 2003.

[2] Lidong Zhou and Zygmunt J. Hass, Securing Ad Hoc Networks, IEEE Networks [3]Special Issue on Network Security, November/December 1999.

[3] Yongguang Zhang and Wenke Lee, Security in Mobile Ad-Hoc Networks, in Book Ad Hoc Networks Technologies and Protocols (Chapter 9), Springer, 2005.

[4] Ad hoc On Demand Distance Vector Routing , Charles E. Perkins, Elizabeth M . Royer, Dept. of Electrical and Computer Engineering, Santa Barbara . CA

[5] ODAR: On-Demand Anonymous Routing in Ad Hoc Networks Denh Sy, Rex Chen and Lichun Bao Bren School of Information and Computer Sciences and Calit2 University of California, Irvine, CA 92697 Emails: {dsy, rex, and lbao}@ics.uci.edu

[6] C. Castelluccia and P. Mutaf. Hash-Based Dynamic Source Routing. In IFIP Networking, LNCS 3042, pages 1012–23, 2004.

[7] D.B. Johnson and D.A. Maltz. Mobile Computing, chapter Dynamic Source Routing in Ad Hoc Wireless Networks, pages153–181. Kluwer Academic Publishers, 1996.

[8] Authenticated Routing for Ad Hoc Networks - IEEE Kimaya Sanzgiri, Daniel LaFlamme, Bridget Dahill, Brian Neil Levine, Member, IEEE,

[9] Secure Ad hoc On-Demand Distan Mobile Networks Laboratory Nokia Research Center FIN-00045

[10] SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks Yih-Chun Hu; Johnson, D.B.; Perrig, A.; Rice Univ., Houston, TX .IEEE

[11] Secure Routing for Mobile Ad Hoc Networks . Panagiotis Papadimitratos and Zygmunt J. Haas School of Electrical and Computer Engineering Cornell University, Ithaca, NY 14853, USA http://wnl.ece.cornell.edu

[12] The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad Hoc Networks David B. Johnson David A. Maltz Josh Broch Computer Science Department Carnegie Mellon University Pittsburgh, PA 15213-3891

[13] The Interzone Routing Protocol (IERP) for Ad Hoc Networks Zygmunt J. Haas, Marc R. Pearlman, Prince Samar, Cornell University

[14] Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks YIH-CHUN HU− and ADRIAN PERRIG Carnegie Mellon University, USA DAVID B. JOHNSON Rice University, USA

[15] Security Issues in Mobile Ad Hoc Networks- A SurveyWenjia Li and Anupam Joshi Department of Computer Science and Electrical Engineering University of Maryland, Baltimore County

[16] Security in Ad-hoc Networks Arun Kumar Bayya Siddhartha Gupte Yogesh Kumar Shukla Anil Garikapati

[17] A Review of Current Routing Attacks in Mobile Ad Hoc Networks Rashid Hafeez Khokhar ,Md Asri Ngadi , Satria Mandala Faculty of Computer Science and Information System Department of Computer System & Communication Universiti Teknologi Malaysia (UTM) Skudai, 81310, Johor Bahru, Malaysia

[18] Attack Analysis and Detection for Ad Hoc Routing Protocols Yi-an Huang and Wenke Lee College of Computing Georgia Institute of Technology801 Atlantic Dr. Atlanta, GA, USA 30332

[19] Ad hoc On-Demand Distance Vector Routing Charles E. Perkins Sun Microsystems Laboratories Advanced Development Group Menlo Park ; CA 94025 cperkins@eng.sun.com / Elizabeth M. Royer

[20] C.E. Perkins, E. Royer, and S.R. Das. "*Ad hoc on demand distance vector (AODV) routing*", Internet Draft, March 2000.

[21] C.Siva Ram Murthy and B. S. Manoj. "*Ad hoc wireless networks: Architecture and Protocols"*. Prentice Hall Publishers, May 2004, ISBN 013147023X.

[22] Prabha Ramachandran and Alec Yasinsac. *"Limitations of On Demand Secure Routing Protocols*". Proceedings of the 2003 IEEE Workshop on Information Assurance United States Military Academy, West Point, NY June 2001. http://www.cs.fsu.edu/~yasinsac/Papers/RY04.pdf