ISSN (Online) 2249 - 054 X

International Journal of Computing and Corporate Research

Specialized and Refereed Journal for
Research Scholars, Academicians, Engineers and Scientists

http://www.ijccr.com

International Manuscript ID : ISSN2249054X-V3I3M9-052013

VOLUME 3 ISSUE 3 May 2013

AN EMPIRICAL SURVEY ON DATA SECURITY IN AD-HOC NETWORKING USING MULTIPATH ROUTING

Mane Vijaykumar and Dr. Sohan Garg

Department of Computer Science, **SHRI VENKATESHWARA** University, GAJRAULA, DIST. J.P. NAGAR (U.P.)

Abstract

These days ad-hoc network research has focused on supplying routing services without considering security. In this report, we are providing the information on security threats against ad hoc routing protocols. In light of these threats, we identify three different environments with distinct security requirements. We advise a solution to one; the managed-open scenario where no network substructure is pre-deployed, but prior security coordination is required. Development of hand-held features and mobile telephony makes Ad hoc networks widely adopted, but security remains a complicated issue. Recently, there are several proposed solutions treating authentication, availability, secure routing and intrusion detection etc, in Ad hoc networks. In this report we will analyze some securing data protocol in Ad hoc network. These solutions increase the robustness of transmitted data confidentiality by exploiting the existence of multiple paths between nodes in an Ad hoc network. This report also includes an overview of

current solutions and vulnerabilities and attacks in Ad hoc networks. Ad hoc wireless networks accept no pre-deployed infrastructure is available for routing packets end-to-end in a network, and instead rely on intermediary peers. Securing ad hoc routing presents challenges because each user brings to the network their own mobile unit, without the centralized policy or control of a traditional network. Many ad hoc routing protocols have been proposed

1 INTRODUCTION

An ad hoc network is a collection of wireless mobile hosts making a temporary network without the aid of any established substructure or centralized administration. In such an environment, it may be necessary for one mobile host to enlist the aid of other hosts in forwarding a packet to its destination, due to the limited range of each mobile host's wireless transmissions. Mobile ad hoc networks (MANET) do not rely on any fixed infrastructure but communicate in a self-organized way.

1.1 Data Security Aims

1) **Availability:** Ascertains survivability despite Denial of Service (DOS) attacks. On physical and media access control layer attacker can use jamming techniques to interfere with communication on physical channel. On network layer the attacker can disrupt the routing protocol. On higher layers, the attacker could bring down high level services e.g.: key management service.

2) **Secure routing:** Ascertains certain information is never exposed to unauthorized entities.

3) **Integrity:** Message being transmitted is never corrupted.

4) **Authentication:** Enables a node to ascertain the identity of the peer node it is communicating with. Without which an attacker would impersonate a node, thus gaining unauthorized access to resource and sensitive information and interfering with operation of other nodes.

5) **Non-repudiation:** Ensures that the origin of a message cannot deny having sent the message.

1.2 Challenges

Use of wireless links renders an Ad hoc network susceptible to link attacks ranging from passive listening in to active personating, message replay and message distortion. Listening in might give an attacker access to secret information thus offend confidentiality. Active attacks could range from deleting messages, injecting erroneous messages; impersonate a node etc thus violating availability, integrity, authentication and non-repudiation. Nodes roaming freely in a hostile environment with relatively poor physical protection have non-negligible probability of being compromised. Hence, we need to consider malicious attacks not only from outside but also from within the network from compromised nodes. For high survivability Ad hoc networks should have a distributed architecture with no central entities, centrality increases vulnerability. Ad-hoc network is dynamic due to frequent changes in topology. Even the trust relationships among individual nodes also changes, especially when some nodes are found to be compromised. Security mechanism need to be on the fly (dynamic) and not static and should be scalable. Hundreds of thousands of nodes.

1.3 Key Management

Cryptographic schemes are often applied to protect both routing info as well as data, for example-digital signatures. Public key systems are generally adopted because of its upper hand in key distribution. In public key substructure each node has a public/private key pair. Public keys distributed to other nodes, while private keys are kept to nodes themselves and that too confidentially. Third party (trusted) called Certification Authority (CA) is used for key management.CA has a public/private key pair, with its public key known to every node and signs certificates binding public keys to nodes. The trusted CA has to stay online to reflect the current bindings, since the bindings could change overtime. Public key should be revoked if the owner node is no longer trusted or is out of network. A single key management service for an Ad-hoc network is probably not a good idea, since it's likely to become Achilles' heel of the network. If CA is down/unavailable nodes cannot get the current public keys of other nodes to establish secure connection. Also if a CA is compromised, the attacker can sign any erroneous certificates with the private key. Naive replication of CA can make the network more vulnerable, since compromising of a single replica can cause the system to fail. Hence it's more prudent to distribute the trust to a set of nodes by letting these nodes share the key management responsibility.

1.3 Secure Routing

The contemporary routing protocols for Ad-hoc networks deal well with dynamically changing topology but are not designed to adapt defense against malicious attackers. No single standard protocol. Capture common security threats and provide guidelines to secure routing protocol. Routers exchange network topology informally in order to establish routes between nodes - another potential target for venomous attackers who intend to bring down the network. External attackers - injecting erroneous routing info, replaying old routing info or distorting routing info in order to partition a network or overloading a network with retransmissions and inefficient routing. Internal compromised nodes - more severe detection and correction more difficult Routing info signed by each node won't work since compromised nodes can generate valid signatures using their private keys. Detection of compromised nodes through routing information is also difficult due to dynamic topology of Ad-hoc networks. Can make use of some properties of ad-hoc networks to facilitate secure routing. Routing protocols for Ad-hoc networks must handle outdated routing information to accommodate dynamic changing topology. False routing information generated by compromised nodes can also be regarded as outdated routing information. As long as there are sufficient no. of valid nodes, the routing protocol should be able to bypass the compromised nodes, this however needs the existence of multiple, possibly disjoint routes between nodes. Routing protocol should be able to make use of an alternate route if the existing one appears to have faulted.

2. SYSTEM ARCHITECTURE AND MAJOR DESIGN ISSUES

2.1. Threshold Secret Sharing

The first issue is how to divide the message into multiple parts? Simply hacking the message into multiple segments involves the least processing overhead. However, it does not provide extra security protection. Since each segment contains partial content of the message, which might be used to derive the content of the entire message. It is also difficult to protect the integrity of the message. In our SPREAD scheme, we use the threshold secret sharing algorithm to divide the secret message into multiple parts. Threshold secret sharing algorithms could divide a secret into N pieces, called shares or shadows. From any less than T shares one cannot learn anything about the system secret, while with an efficient algorithm, one can reconstruct the system secret from any T out of N shares. This is called a (T, N) threshold secret sharing scheme. Thus with a (T,N) secret sharing algorithm, the secret message can be divided into N message shares such that in order to compromise the message, the enemy has to compromise at least T shares. With less than the threshold, namely T, shares, the enemy could learn nothing about the message and has no better chance to recover the secret than an outsider who knows nothing at all about the message. This gives us the desired security properties. Another reason that we use secret sharing is that the generation of the message shares and the reconstruction of the message are all linear operations over a finite field (Shamir's Lagrange interpolating polynomial scheme). In addition, the secret sharing scheme can be designed with cheating detection and cheater identification. It is possible that after compromising a node, the adversary may attempt to cheat our system by sending us the faked or altered message shares. By embedding the cheater detection and identification, we can deterministically detect cheating and identify the cheater, no matter how many cheating shares are involved in the secret reconstruction. This is a very useful detection mechanism in an unreliable ad hoc network environment and helps to protect the integrity of the message transmitted.

2.2. **Share Allocation**

The second issue is how to select the paths, how to choose an appropriate value of (T, N), and how to allocate the shares onto each selected path such that the maximum security can be achieved. We consider the case that a message is compromised due to compromised nodes. We accept that if a node is compromised, all the credentials of that node will be compromised. So the message shares traveling through that node are all bugged and recovered. Given the available independent paths and their corresponding security characteristics, the fundamental objective is to maximize the security by allocating the shares in such a way that the opponent has to compromise all the paths to recover the message. The merest and most intuitive share allocation scheme is to choose N as the number of available paths, apply (N, N) secret sharing, and allocate one share onto each path. This will achieve the desired maximum security with least processing cost. However, in an ad hoc network, wireless links are instable and the topology changes frequently. Sometimes packets might be cut down due to the bad wireless channel condition, the collision at MAC layer transmission, or stale routing information. In the case that packet loss does occur, this type of non-redundant share allocation will disable the reconstruction of the message at the proposed destination. To deal with this problem, it is usually necessary to introduce some redundancy (i.e. T<N) in the SPREAD scheme to improve the reliability, i.e. the destination would have better chance to receive enough shares for reconstructing the message. Usually speaking, security and reliability are two contradictive design goals - more redundancy involves better reliability but worse security. However, due to the salient feature of the threshold secret sharing, we develop the redundant SPREAD share allocation which could tolerate certain packet losses while at the same time maintain the maximum security, i.e. forcing the opponent to compromise all the paths to compromise the message. We formulate the share allocation into a constrained optimization problem, with the objective to minimize the message compromise probability. Our probing to the optimum share allocation reveals that, by choosing an appropriate (T,N) value and allocating the shares onto each path carefully, we could improve the reliability by enduring certain packet loss without giving the security. The maximum redundancy we can add to the SPREAD scheme without sacrificing security is identified. The optimal share allocation is proposed.

3.3. **Multipath Routing and Path Set Optimization**

Third one is the multipath routing in ad hoc networks – how to find the desired multiple paths in a mobile ad hoc network and how to deliver the shares to the destination using these paths?

Routing in a MANET presents great challenge because the nodes are capable of moving and the network topology can change continuously, dramatically and erratically. A great effort has been made in designing ad hoc routing protocols in response to the frequent topological changes. Multipath routing technique is a promising choice since the use of multiple paths in a MANET could diminish the effect of unreliable wireless links and the frequent topological changes. Several multipath routing schemes have been proposed to improve the reliability, fault-tolerance, end-to-end delay for eruptive traffic, as well as to achieve load balancing. For our SPREAD scheme, we need independent paths, more specifically, node disjoint paths, because we are dealing with node compromising problem. Several multipath routing protocols have been proposed in MANETs with the design goal to find node-disjoint paths, such as the split multipath routing , the variety injection technique, and the on demand multipath routing . The dynamic source routing (DSR) protocol itself is also capable of maintaining multiple paths from the source to a destination. Those proposed protocols are all on-demand, due to the network bandwidth limitation, and source routing type, as the source routing provides the source with the maximal capability of controlling the disjointness of the paths. Those on-demand protocols work by broadcasting the route inquiry messages throughout the network and then gathering the replies from the destination. Although those routing protocols are able to find multiple node-disjoint paths, the paths found directly by them might not be optimal for our SPREAD scheme as the path selection is usually based on the hop count or propagation delay, not necessary the security. For our SPREAD scheme, we take a similar on-demand and source routing type of approach. However, we make use of the "link cache" organization we proposed in where each path returned to source is decomposed into individual links and represented in a unified graph data structure. Using such a link cache organization allows us to further optimize the path set used for SPREAD. Although we rely on an underlying routing protocol to provide us with a partial view of network topology, the optimization of the path set can be done solely based on the discovered partial network topology, which is independent of the underlying routing protocols. For the optimization of the paths, we propose a security related link cost function such that the path can be found according to their security level (i.e. the probability that the path might be compromised). Then, we apply a maximal node disjoint path finding algorithm to discover as many paths as possible and at the same time as secure as possible.

3. VULNERABILITIES AND ATTACKS IN AD HOC NETWORKS

In security field, new exposures appear with Ad hoc technology. Nodes become easier to be slipped since they are mobile, the computing capacity is limited. That makes using heavy solutions, as PKI, not very practice. Also, Ad hoc networks services are tentative and batteries are a limited feeding resource what makes a Denial of Service attack by consumption of energy very possible.

Ad hoc networks are exhibited to many possible attacks. We can classify these attacks into two kinds: Passive attacks and Active attacks.

In passive attacks, assailants don’t break up the operation of routing protocol but only attempt to discover valuable information by listening to the routing traffic. Defending against such attacks is difficult, because it is usually impossible to detect listening in a wireless environment. Furthermore, routing information can reveal relationships between nodes or disclose their IP addresses.

If a route to a particular node is requested more often than to other nodes, the assailants might expect that the node is important for the functioning of the network, and disabling it could bring the entire network down. While passive assails are rarely detectable, active ones can often be detected.

An active assail can mainly be:

a) Black hole assails. A venomous node uses the routing protocol to push itself as having the shortest path to the node whose packets it wants to intercept.

b) Wormhole assails. In this type of attacks, an assailant’s records packet at one location in the network, tunnels them to another location, and retransmits them there into the network. This attack is possible even if the attacker has not compromised any hosts and even if all communication provides authenticity and confidentiality.

c) Routing tables overflow assails. Here the assailant attempts to create routes to Nonexistent nodes. The goal is to create enough routes to prevent new routes from being created or to overwhelm the protocol implementation. It seems that proactive algorithms are more vulnerable to table overflow attacks than reactive algorithms because they attempt to discover routing information every time.

d) Sleep privation attacks. Because battery life is a critical parameter in Ad hoc networks, devices try to conserve energy by transmitting only when necessary. An assailant can attempt to consume batteries by requesting routes, or by forwarding necessary packets to the node using, for example, a black hole attack.

e) Location disclosure assails. It's an attack which can reveal something about the nodes location or the structure of the network. The attack can be as simple as using an equivalent of the trace route command on UNIX systems. In this attack, the attacker knows which nodes are situated on the route to the target node.

f) Denial of service assails. Such attacks, generally, flood the network making it crashing or engorged. Also, wormhole, routing table overflow and sleep privation attacks might fall into this attacks category.

g) Impersonation attacks. If authentication is not supported, compromised nodes may be able to send false routing information, masqueraded as some others, etc.

4. SECURING DATA BASED MULTIPATH ROUTING IN AD HOC NETWORKS

The protocol consists of separating the initial message and overworking the characteristic of existence of multiple paths between nodes in an Ad hoc network to increase the lustiness of confidentiality. In our solution, even if an assailant succeeds to have one or lots of transmitted parts, the probability of original message reconstruction is low.

4.1. Principle

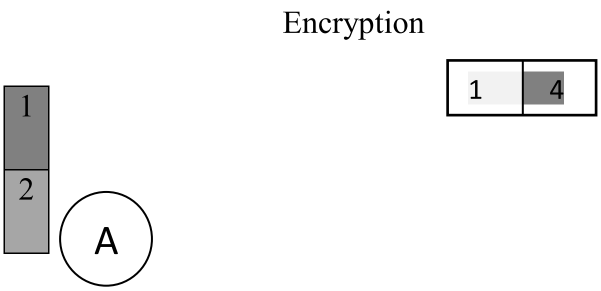
At first, we present the principle of Secured Data based Multipath method in a simplified scheme in Fig.1, and then we expose with details how it works. We do not modify the existing lower layers protocols. We have the following suppositions:

(1) The sender ‘A’ and the receiver ‘B’ are authenticated.

(2) WEP is used for the encryption/decryption of all the frames at MAC layer and the authentication of the terminals.

(3) A mechanism of discovering the topology of the network is available.

(4) And the used routing protocol supports multi-routes.



ISSN (Online) 2249 - 054 X
International Journal of Computing and Corporate Research
Specialized and Refereed Journal for
Research Scholars, Academicians, Engineers and Scientists

http://www.ijccr.com

International Manuscript ID : ISSN2249054X-V3I3M9-052013

VOLUME 3 ISSUE 3 May 2013

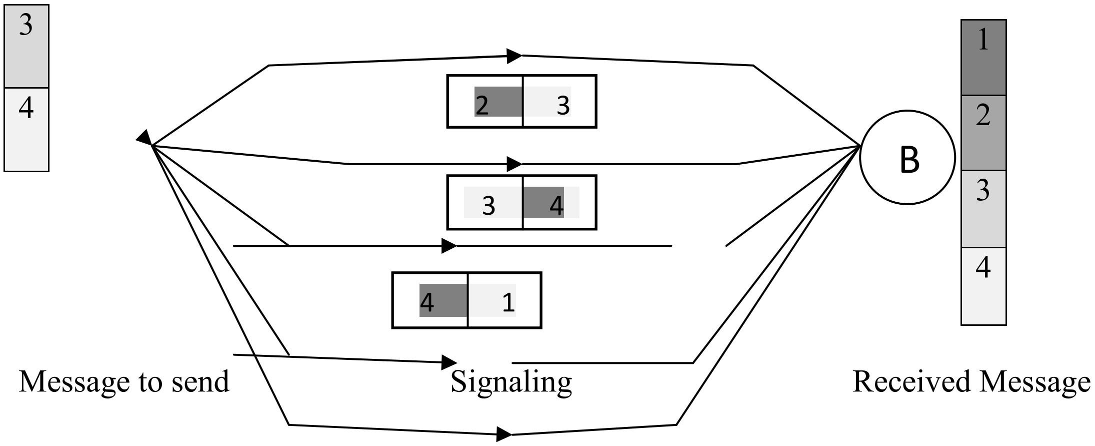


Figure 1. Principle of the proposed solution

The protocol we suggest starts by taking into retainer the network topology. It uses n routes (n ≥ 3) among N available ones existing between the sender and the receiver. We distinguish between two types of channels. The first type is committed only for signaling. The second contains user data. The first type needs one link and the second (n-1) ones. For this reasons, we should have at least 3 links. With only two, our initial message can't be divided into shares. The original message m is divided into (n-1) parts; each of them has a unique identifier. The protocol generates, then, a random number x (1< x ≤ (n-1), x integer) to be sent on one of the n paths (what we called signaling channel), then codes parts in pairs using an XOR operation related to x. Every combination is sent over one of the (n-1) channels. The xth part is sent in plain text. It will be the start point for receiver to find other parts. Concerning the manner of dividing messages, a channel coding approach called Diversity Coding used for self-healing and fault permissiveness in digital communication networks for nearly instantaneous recovery from link failures can be used.

B. Algorithm description

We first introduce the terminology we used to express our method algorithm.

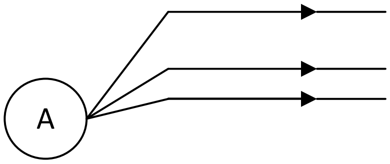
- m: message to be sent secured between A and B. Dividing m into n-1 parts gives: P (m) = {c1, c2, …, c n-1}
- Tp (ntwk): Function called every t= frequency to discover topology of the Ad hoc network. Returns true if modifications in topology, else, it returns false.
- Frequency: frequency of topology refreshing.
- N (A,B) : number of links between A and B
- n: integer; 3 ≤ n ≤ N(A,B)

Part 1

```
Input: (network topology, m)
Tp(ntwk) = true
While (connection is active)
{
if ( Tp (ntwk) == true )
{
        if ( N(A,B) ≥ 3 )
        {
            take n links among N(A,B)
            divide m into n-1 parts to form P (m) = {c1, c2, …, c n-1}
            generate x randomly (x integer/ 1< x ≤ (n-1))
        }
        Output: P (m) = {c1, c2,… c n-1}, x
        Wait (frequency)
    }
}
```

Part 2

We combine, then, the n-1 parts of m in pairs on every path using an XOR operation related to x. On the nth link, we send values of x and n. Combination algorithm is done as it follows in the scheme below:



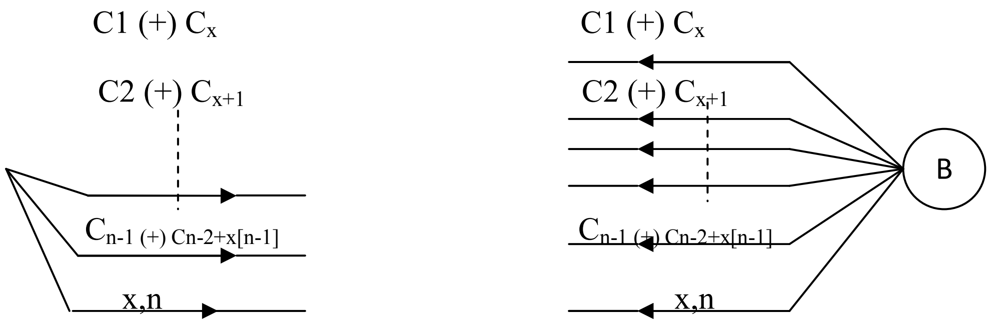


Figure 2. Second step of the method

Results of the combination of every pair of message parts on every data channel are sent encrypted by WEP to reinforce confidentiality. This gives a double shielding to the message to transmit securely. Parts' identifiers are sent to allow the receiver to reconstitute the original message in order. For fault tolerance problem, we can also use Diversity Coding technique which is based on information redundancy. Even if an attacker succeeds to have one or lots of transmitted parts, the probability of message reconstruction is low. The attacker must have all the parts. This means that he/she has to eavesdrop on all used channels or should be near A or B location. In addition to this, he/she should know our combining function and be able to decrypt the WEP encoding, which are hard tasks, or almost impossible to do at the same time.

D. Architecture

Our algorithm can be run with both reactive and proactive routing protocols. We add a layer situated on top of the transport (TCP/UDP) one that will manage the use of our solution to secure sent data. Specific header, called SDMP (Secured Data based Multipath) header will be added for useful information to assure security. The Secured Data based Multipath (SDMP) protocol introduces a set of features that can be incorporated with low overhead without modifying low layers protocols. Both sender and receiver should use SDMP layer to be able to use this protocol.

APP
SDMP
TCP/UDP
IP
LINK
PHY

Figure 4. New Protocol Stack

The SDMP protocol needs to transfer some information to ensure running of the proposed security solution. SDMP header contains six fields, as shown in Fig. 4:

Flag	Seq num	Attempt num	Rem adr num	IP address num	Combined Data

Figure 5. SDMP packet Format

Flag: to denote nature of SDMP packet (plaintext data or XOR combination).

• Seq num: to identify sent fragments.

• Attempt num: for retransmission management.

• Rem adr num: number of nodes remained to pass by.

• IP adr list: contains IP addresses of nodes to pass by to reach destination.

• Combined data: fragments combination result.

The first entry needed is the network topology to define which routes link A to B. The source node A initiates this operation. When the routing protocol returns detected topology, SDMP protocol calculates N, the number of routes linking A to B. If N is < 3, it generates an error message, else the n routes it will use to transmit data securely will be chosen among the N ones according to a cost function as transit delay. SDMP protocol restructures, at receiver side, message parts consecutively. So, at sender side, it sends data on the n chosen routes according to the cost function such as receiver side spends minimal time to restructure original parts. Values of x and n are sent on the signaling channel. SDMP protocol runs continually the algorithm explained above, therefore when topology changes, affected routes have to be notified and data is retransmitted. Since paths breakage detection depends on the chosen refreshing frequency, SDMP protocol can calculates it at the beginning according to the network mobility.

ISSN (Online) 2249 - 054 X

International Journal of Computing and Corporate Research

Specialized and Refereed Journal for
Research Scholars, Academicians, Engineers and Scientists

http://www.ijccr.com

International Manuscript ID : ISSN2249054X-V3I3M9-052013

VOLUME 3 ISSUE 3 May 2013

ISSN (Online) 2249 - 054 X

International Journal of Computing and Corporate Research

Specialized and Refereed Journal for
Research Scholars, Academicians, Engineers and Scientists

http://www.ijccr.com

International Manuscript ID : ISSN2249054X-V3I3M9-052013

VOLUME 3 ISSUE 3 May 2013

REFERENCES:

[1] B. Shrader, "A proposed definition of Ad hoc network," Royal Institute of Technology (KTH), Stockholm, Sweden, May 2002.

[2] M. M. Lehmus, "Requirements of Ad hoc Network Protocols," Technical report, Electrical Engineering, Helsinki University of Technology, May 2000.

[3] A. Qayyum, "Analysis and evaluation of channel access schemes and routing protocols for wireless networks," Ph.D. Dep Computer Science, Paris XI. Paris Sud University, Nov 2000.

[4] W.Diffie, M. Hellman, "New Directions in Cryptography," IEEE Transactions on Information Theory, vol. IT-22(6), pp. 644-654, November 1976

[5] P. Gutmann, "PKI: It's Not Dead, Just Resting," IEEE Computer, pp. 41- 49, August 2002.

[6] http://www.cert.org/tech_tips/denial_of_service.html

[7] Q. Lu, "Vulnerability of Wireless Routing Protocols," Technical Report, University of Massachusetts Amherst, Dec 2002.

[8] H. Li, Z. Chen, X. Qin, C. Li, H. Tan, "Secure Routing in Wired Networks and Wireless Ad Hoc Networks," Technical Report, Department of Computer Science, University of Kentucky, April 2002.

[9] F. Wang, B. Vetter, and S. Wu, "Secure Routing Protocols: Theory and Practice," Technical Report, North Carolina State University, May 1997. [10] Y. Hu and A. Perrig and D. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," in Proc of the Eighth Annual International Conference on Mobile Computing and Networking (MobiCom 2002), pp. 12-23, ACM, Atlanta, GA, September 2002.

[11] F. Stajano and R. Anderson. “The Resurrecting Duckling: Security Issues for Ad hoc Wireless Networks,” in Proc 1999, pp. 172-194.

[12] N. Ahuja and A. Menon, “Security in Mobile Networks : Ad-hoc and Infrastructure,” Computer and Information Sciences, University of Florida, Dec 2001.

[13] H.Hansén, “IPsec and Mobile-IP in Mobile Ad hoc Networking,” April 2000.

[14] http://www.wireless-fr.org/b002_norme80211b.html

[15] A. Abdul-Rahman and S. Hailes, “A Distributed Trust Model,” in Proc 97 New security paradigms, Langdale, Cumbria, United Kingdom, Sep 23-26 1997, pp. 48-60.

[16] N. Asokan and P.Ginzboorg, “Key Agreement in Ad hoc Networks,” Computer Communications, vol. 23(17), pp. 1627-1637, 2000.

[17] F. Stajano, “The Resurrecting Duckling—What Next?,” in Proc 8th Security Protocols Workshop, Lecture Notes in Computer Science 2133, Springer- Verlag, Berlin, 2001, pp. 204–214.

[18] Y. Desmedt, “Threshold Cryptography,” In CRYPTO '89, vol. 435 of LNCS, pp. 307-315, Springer-Verlag, 1990.

[19] L. Zhou and Z. J. Haas, “Securing Ad hoc Networks,” IEEE Network, vol. 13(6), pp. 24-30, 1999.

[20] M. G. Zapata, “Secure Ad hoc On-Demand Distance Vector Routing,” ACM Mobile Computing and Communications Review (MC2R), vol. 6(3), pp. 106-107, July 2002.

ISSN (Online) 2249 - 054 X

International Journal of Computing and Corporate Research

Specialized and Refereed Journal for
Research Scholars, Academicians, Engineers and Scientists

http://www.ijccr.com

International Manuscript ID : ISSN2249054X-V3I3M9-052013

VOLUME 3 ISSUE 3 May 2013

Department of Compute Science**, SHRI VENKATESHWARA University GAJRAULA, DISTT. J.P. NAGAR (U.P.)**