Security in Ad-hoc Networks

Manisha[*], Chanchal[*], Pawan Bhadana[**], Ritu Khurana[**]

[*] Computer Science & Engineering, B.S.A. Institute of Technology & Management, Faridabad, India
[**] Department of Computer Engineering, B.S.A. Institute of Technology & Management, Faridabad, India

Abstract- Ad-hoc networks are an emerging area of mobile computing. There are various challenges that are faced in the Ad-hoc environment. In this paper we attempt to analyze the demands of Ad-hoc environment. We focus on three areas of Ad-hoc networks, key exchange and management, Ad-hoc routing, and intrusion detection. The key issues concerning these areas have been addressed here. We have tried to compile solutions to these problems that have been active areas of research.

Index Terms- Ad-hoc, Routing, Intrusion, Wireless, Key.

I. INTRODUCTION

Ad-hoc networks are a new paradigm of wireless communication for mobile hosts. No fixed infrastructure such as base stations as mobile switching .Nodes within each other radio range communicate directly via wireless links while these which are far apart rely on other nodes to relay messages. Node mobility causes frequent changes in topology.

1.1 Security Goals

1) Availability
2) Confidentiality
3) Integrity
4) Authentication
5) Non-repudiation

1.2 Challenges

Use of wireless links renders an Adhoc network susceptible to link attacks ranging from passive eavesdropping to active impersonation, message replay and message distortion. Hence, we need to consider malicious attacks not only from outside but also from within the network from compromised nodes.

1.3 Key Management

Cryptographic schemes such as digital signatures are often employed to protect both routing info as well as data. Public key systems are generally espoused because of its upper hand in key distribution. Third party (trusted) called Certification Authority (CA) is used for key management.

II. KEY AGREEMENT IN WIRELESS AD-HOC NETWORKS

2.1 New key agreement scenario

Consider a group of people getting together for an Adhoc meeting in a room and trying to establish a wireless network through their laptops. They trust one another personally, however don't have any a priori shared secret (password) to authenticate one another. They don't want anybody outside the room to get a wind of their conversation indoors. This particular scenario is vulnerable to any attacker who not only can monitor the communication but can also modify the messages and can also insert messages and make them appear to have come from somebody inside the room. This is a classic example of Adhoc network and the most simple way to tackle this example would be through location based key agreement - to map locations to name ladles and then use identity based mechanisms for key agreement. e.g.: participants writing the IP addresses on a piece of paper and passing it around. Then a certificate based key agreement mechanism can be used. These public key certificates can allow participants to verify the binding between the IP address and keys of other participants.

Two obvious problems

a) Difficult to determine if the certificate presented by the participant has been revoked.
b) Participants may be divided into 2 or more certification hierarchies and that they don't have cross certification hierarchies.

<u>One obvious solution</u>

A trusted third party capable of locating players, however not always feasible due to non-infrastructure nature of Adhoc networks.

2.2 Password based Authenticated Key Exchange

A fresh password is chosen and shared among those present in the room in order to capture the existing shared context. If this password is a long random string, can be used to setup security association, but less user friendly.

2.3 Password authenticated Diffie - Hellman key exchange

2.3.1 Two party version

In the elementary DH protocol, *two parties* A and B agree on a prime p and a generator g of the multiplicative group Zp* (i.e. the set {1, 2, …, p-1}). A and B choose random secrets SA and SB such that $1 <= S_A, S_B <= p-1$.

(1) A computes g^{SA}, encrypts it with the shared secret password P and sends it to B.
A --> B : A, $P(g^{SA})$.

(2) B extracts g^{SA} from the message computes g^{SB} and also computes the session key $K = (g^{SA})^{SB}$. B then chooses a random challenge C_B and encrypts it using the key K. B encrypts S_B using P. It then sends the two quantities to A.
B --> A : $P(S_B)$, $K(C_B)$.

(3) A extracts S_B from $P(S_B)$ and computes the key $K = (g^{SA})^{SB}$. It then extracts C_B by decrypting $K(C_B)$. A then generates challenge (random) C_A, encrypts both C_A and C_B with K and sends it to B.
A --> B : $K(C_A, C_B)$.

(4) This message(3) convinces B that A was able to decrypt the message in (2) correctly. B then encrypts C_A using K and sends it to A.
B --> A : $K(C_A)$.

A decrypts the message to see if the plaintext is indeed C_A. This would convince A that B knew K. This would in turn convince A that B knew P.

2.3.2 Multi-party version

There are let's just say n players M_1, M_2, …, M_n who all share a password P, each generating a random quantity Si which is its contribution to the eventual session key $K = g^{S1S2\_\_\_Sn\text{-}1Sn}$.

III. SECURE ROUTING IN AD-HOC NETWORKS

3.1 Problems associated with Ad-hoc routing

3.1.1 Infrastructure

An Ad-hoc network is an infrastructure less network. Unlike traditional networks there is no pre-deployed infrastructure such as centrally administered routers or strict policy for supporting end-to-end routing

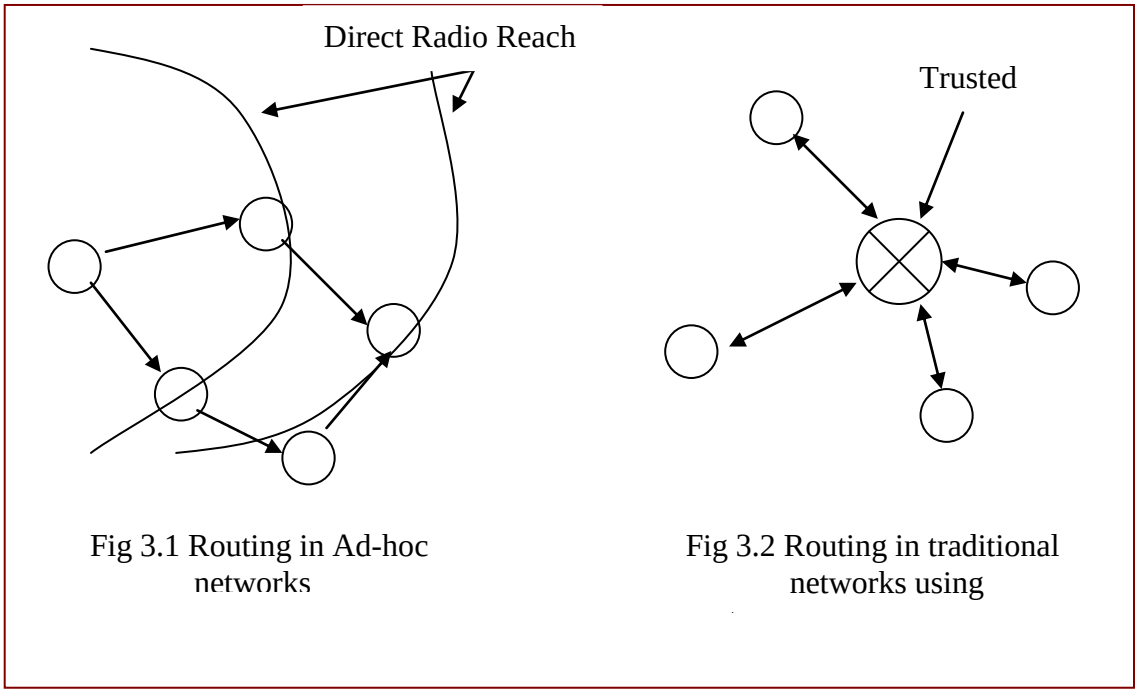


Fig 3.1 Routing in Ad-hoc networks

Fig 3.2 Routing in traditional networks using

3.1.2 Frequent changes in network topology

Ad-hoc networks contain nodes that may frequently change their locations. Hence the topology in these networks is highly dynamic. This results in frequently changing neighbors on whom a node relies for routing.

3.1.3 Problems associated with wireless communication

As the communication is through wireless medium, it is possible for any intruder to tap the communication easily. Routing protocols should be well adopted to handle such problems.

3.1.4 Problems with existing Ad-hoc routing protocols

3.1.4.1 Implicit trust relationship between neighbors

Current Ad-hoc routing protocols inherently trust all participants. Most Ad-hoc routing protocols are cooperative by nature and depend on neighboring nodes to route packets. This naive trust model allows malicious nodes to paralyze an Ad-hoc network by inserting erroneous routing updates, replaying old messages, changing routing updates or advertising incorrect routing information. While these attacks are possible in fixed network as well, the Ad-hoc environment magnifies this makes detection difficult.

3.1.4.2 Throughput

Ad-hoc networks maximize total network throughput by using all available nodes for routing and forwarding. However a node may misbehave by agreeing to forward packets and then failing to do so, because it is overloaded, selfish, malicious or broken. Misbehaving nodes can be a significant problem.

3.1.4.3 Attacks using modification of protocol fields of messages

Current routing protocols assume that nodes do not alter the protocol fields of messages passed among nodes. Routing protocol packets carry important control information that governs the behavior of data transmission in Ad-hoc networks. Since the level of trust in a traditional Ad-hoc network cannot be measured or enforced, enemy nodes or compromised nodes may participate directly in the route discovery and may intercept and filter routing protocol packets to disrupt communication. Malicious

nodes can easily cause redirection of network traffic and DOS attacks by simply altering these fields.

3.1.5 Attacks using impersonation

Current Ad-hoc routing protocols do not authenticate source IP address. A malicious node can launch many attacks by altering its MAC or IP address. Both AODV and DSR are susceptible to this attack.

3.1.6 Attacks using fabrication

Generation of false routing messages is termed as fabrication messages. Such attacks are difficult to detect.

3.1.7 No way to detect and isolate misbehaving nodes

misbehaving nodes can affect network throughput adversely in worst-case scenarios. The existing Ad-hoc routing protocols do not include any mechanism to identify misbehaving nodes.

3.1.8 Easily leak information about network topology

Ad-hoc routing protocols like AODV and DSR carry routes discovery packets in clear text. These packets contain the routes to be followed by a packet. By analyzing these packets any intruder can find out the structure of the network.

3.1.9 Lack of self-stabilization property

Routing protocols should be able to recover from an attack in finite time. An intruder should not be able to permanently disable a network by injecting a smaller number of mal-informed routing packets

3.2 Solutions to problems in Ad-hoc-routing

3.2.1 Using pre-deployed security infrastructure

Here we assume existence of certain amount of security infrastructure. The type of Ad-hoc environment that we are dealing with here is called managed-open environment.

Assumptions

A managed-open environment assumes that there is opportunity for pre-deployment. Nodes wishing to communicate can exchange initialization parameters before hand, perhaps within the security of an infrastructured network where session keys may be exchanged or through a trusted third party like a certification authority.

ARAN protocol in managed-open environment

ARAN or Authenticated Routing for Ad-hoc Networks detects and protects against malicious actions by third parties and peers in Ad-hoc environment. ARAN introduces authentication, message integrity and non-repudiation to an Ad-hoc environment.

ARAN is composed of two distinct stages. The first stage is simple and requires little extra work from peers beyond traditional ad hoc protocols. Nodes that perform the optional second stage increase the security of their route, but incur additional cost for their ad hoc peers who may not comply (e.g., if they are low on battery resources).

ARAN makes use of cryptographic certificates for the purposes of authentication and non-repudiation.

Route Maintenance

ARAN is an on-demand protocol. Nodes keep track of whether routes are active. When no traffic has occurred on an existing route for that route's lifetime, the route is simply de-activated in the route table. Data received on an inactive route causes nodes to generate an Error (ERR) message that travels the reverse path towards the source. Nodes also use ERR messages to report links in active routes that are broken due to node movement. All ERR message must be signed.

Key revocation

ARAN attempts a best effort key revocation that is backed up with limited time certificates. In the event that a certificate needs to be revoked, the trusted certificate server, T, sends a broadcast message to the ad hoc group that announces the revocation.

3.2.2 Concealing Network topology or structure

1) Using independent Security Agents (SA)

This method is called the Non-disclosure method (NDM). In NDM a number of independent security agents (SA) are distributed over the network. Each of these agents SA_i owns a pair of asymmetric cryptographic keys K_{SAi} and K_{SAi}-. Sender s wishes to transmit a message M to receiver R without disclosing his location. S sends the message using a number of SAs: $SA_1 \rightarrow SA_2 \rightarrow \ldots \rightarrow SA_N \rightarrow$ R. The message is encapsulated N times using the public keys $K_{SA1} \ldots K_{SAn}$

To deliver the packet, S sends it to the first security agent SA_1 which decrypts the outer most encapsulation and forwards the packet to the next agent. Each SA knows only the address of the previous and the next hop. The last agent finally decrypts the message and forwards it to R. It introduces a large amount of overhead and hence is not preferred for routing.

2) Zone Routing Protocol (ZRP)

It is a hierarchical protocol where the network is divided in to zones. The zones operate independently from each other. ZRP involves two separate routing protocols.

Such a hierarchical routing structure is favorable with respect to security since a well designed algorithm should be able to contain certain problems to small portion of the hierarchy leaving other portions unaffected.

3.2.3. Installing extra facilities in the network to mitigate routing misbehavior

Misbehaving nodes can reduce network throughput and result in poor robustness. Sergio Marti Et al propose a technique to identify and isolate such nodes by installing a watchdog and a pathrater in the Ad-hoc network on each node.

Assumptions

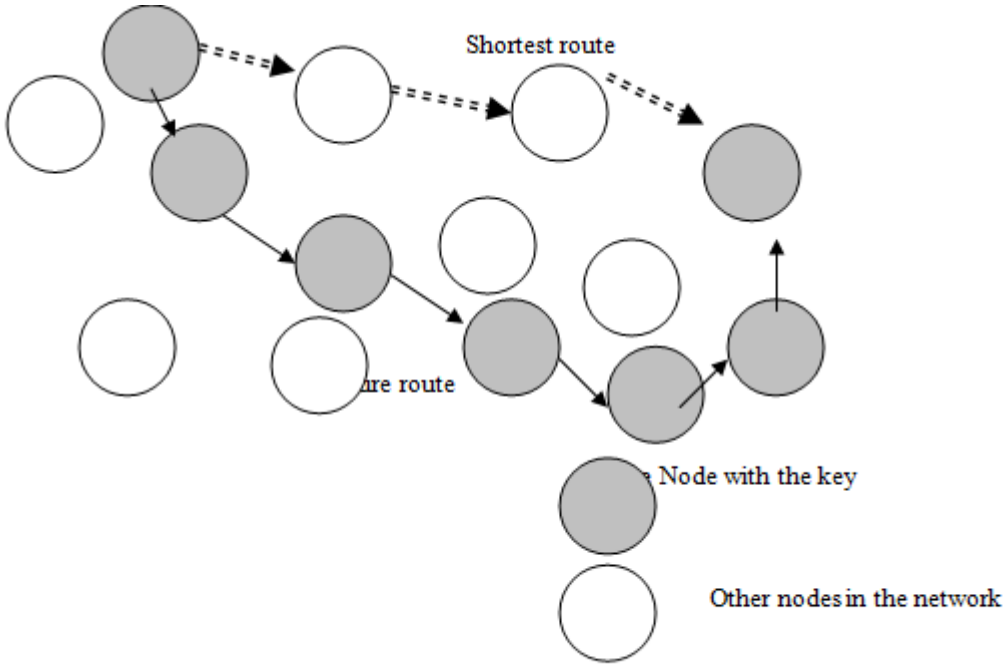
It is assumed that the wireless links are bi-directional. Most MAC layer protocols require this. It also assumes support for promiscuous mode of operation for the nodes. This helps the nodes supervise each other operation. The third assumption is that the underlying Ad-hoc routing protocol is DSR. It is possible to extend the mechanism to other routing protocols as well.

Mechanism

The watchdog identifies misbehaving nodes, while the pathrater avoids routing packets through these nodes. When a node forwards a packet, the node's watchdog verifies that the next node in the path also forwards the packet. The watchdog does this by listening promiscuously to the next node's transmissions. If the next node does not forward the packet, then it is misbehaving. The pathrater uses this knowledge of misbehaving nodes to choose the network path that is most likely to deliver packets.

3.2.4 Security-Aware Ad-hoc Routing (SAR)

It makes use of trust levels (security attributes assigned to nodes) to make informed, secure routing decision. Current routing protocols discover the shortest path between two nodes. But SAR can discover a path with desired security attributes (E.g. a path through nodes with a particular shared key).



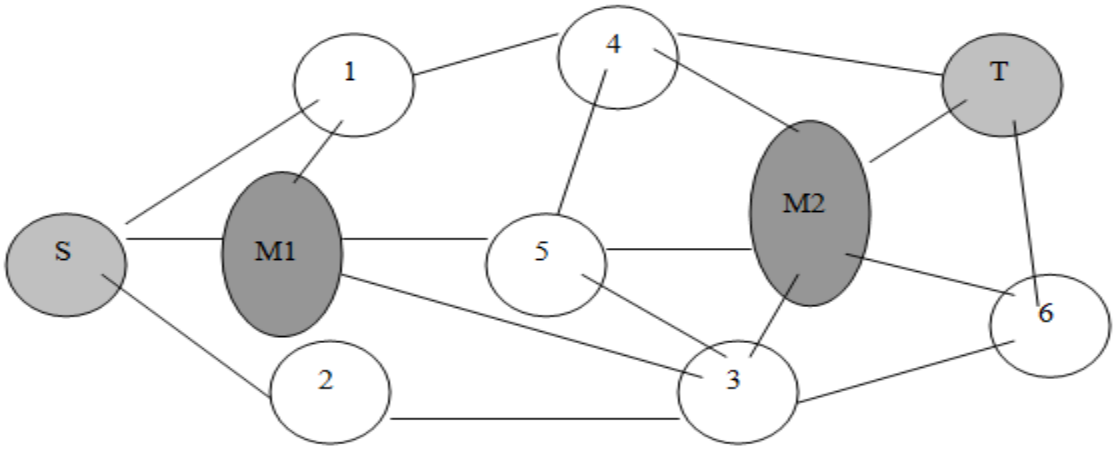
3.2.5 Secure Routing Protocol

3.2.5 Secure Routing Protocol

Assumptions

A Security Association (SA) exists between the source node (S) and destination node (T). The SA would be established by any of group key exchange schemes. However the exists of SAs with any of the intermediate nodes is unnecessary.

Working



The source node (S) initiates the route discovery by constructing a route request packet. The route request packet is identified by a random query identifier (rnd#) and a sequence number (sq#). We assumed that a security association (a shared key K_{ST}) is established between source (S) and destination (T).

S constructs a Message Authentication Code (MAC) which is a hash of source, destination, random query identifier, sequence number and K_{ST}

i.e. MAC = h(S, T, rnd#, sq#, K_{ST}). In addition the identifier (IP addresses) of the traversed intermediate nodes are accumulated in the route request packet.

Intermediate nodes relay route requests. The intermediate nodes also maintain a limited amount of state information regarding relayed queries (by storing their random sequence number), so that previously seen route requests are discarded.

More than one route request packet reaches the destination through different routes. The destination T calculates a MAC covering the route reply contents and then returns the packet to S over the reverse route accumulated in the respective request packet. The destination responds to one or more route request packets to provide the source with an as diverse topology picture as possible.

IV. INTRUSION DETECTION IN WIRELESS AD-HOC NETWORKS

Each node within the network has its own individual IDS agent and these agents run independently and monitor user and system activities as well as communication activities within the radio range. If an anomaly is detected in the local data or if the evidence is inconclusive, IDS agents on the neighboring nodes will cooperatively participate in a global intrusion detection scheme. These individual IDS agents constitute the IDS system to protect the wireless ad-hoc network.

A majority based Intrusion Detection Algorithm can include following steps :

1) The node sends to its neighboring node an "intrusion state request".
2) Each node , including the one which initiates this algorithm then propagates the state information, indicating the likelihood of an intrusion to its immediate neighbors.
3) Each node then determines whether the majority of the received reports point towards an intrusion, if yes then it concludes that the network is under attack.
4) Any node which detects an intrusion to the network can then initiate the remedial/response procedure.

4.5 Anomaly detection in wireless ad-hoc networks

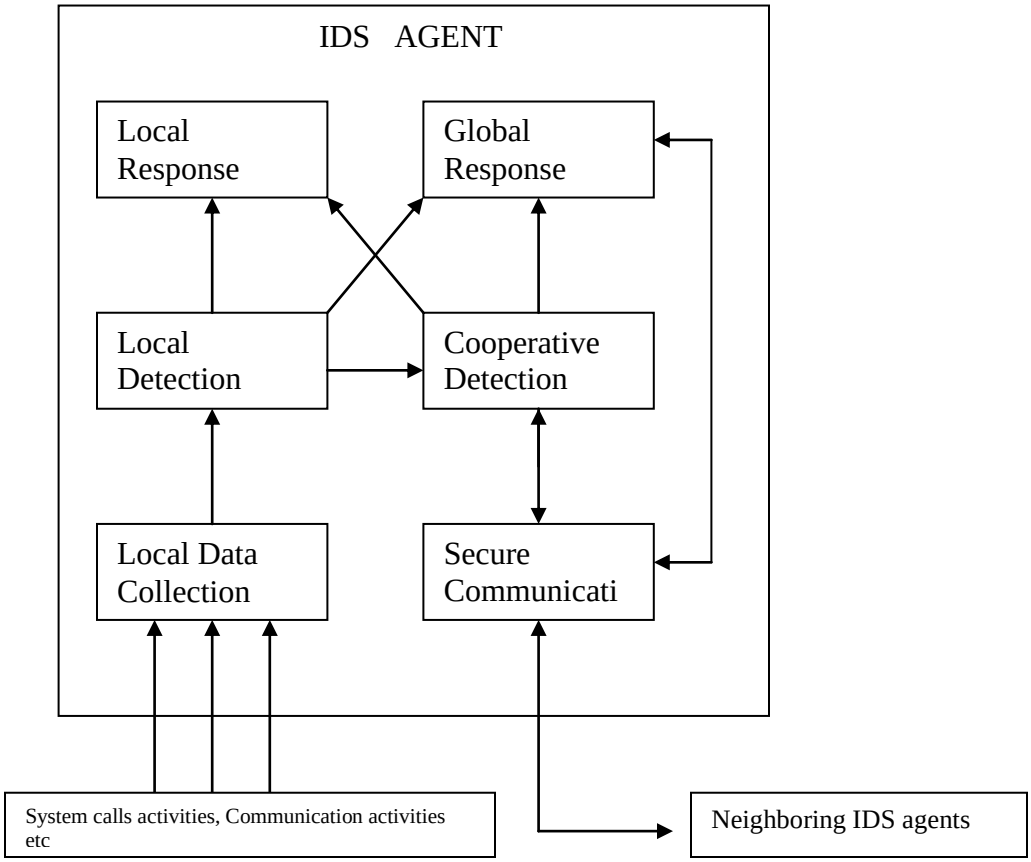
4.5.1 Detecting Abnormal Updates to Routing Tables

A legitimate change in the routing table is caused by physical motion of the nodes or changes in the membership of the network. For a node , it own movement and the change in its own routing table are the only data it can trust and hence we use it as a basis of the trace data. The physical movement is measured by distance , direction and velocity. The routing table change is measured by Percentage of changed routes (PCR), and the percentage changes in the sum of hops of all routes (PCH).

4.5.2 Detecting Anomalous activities in other layers

For MAC protocols , trace data could be in the form of total number of channel requests, the total number of nodes making those requests etc, for last s seconds.

Similarly, at the Wireless Application layer can use service as the class and can contain following features – for the past s seconds, the total number of requests to the same service, total number of services requested, the average duration of service, the number of nodes that requested service, the total number of service errors etc



V. CONCLUSION

We have presented an overview of the existing security scenario in the Ad-Hoc network environment. Key management, Ad-hoc routing and intrusion detection aspects of wireless Ad-hoc networks were discussed. Ad-hoc networking is still a raw area of research as can be seen with the problems that exist in these networks and the emerging solutions. The key management protocols are still very expensive and not fail safe. Several protocols for routing in Ad-hoc networks have been proposed. There is a need to make them more secure and robust to adapt to the demanding requirements of these networks. Intrusion detection is a critical security area. But it is a difficult goal to achieve in the resource deficient Ad-hoc environment. But the flexibility, ease and speed with which these networks can be set up implies they will gain wider application. This leaves Ad-hoc networks wide open for research to meet these demanding application.

REFERENCES

[1] Intrusion Detection in Wireless Ad-hoc Networks, Yongguang Zhang, Wenke Lee

[2] Key Agreement in Ad-hoc Networks, N.Asokan, Philip Ginzboorg

[3] Securing Ad-hoc Networks, L. Zhou, Z.J.Haas

[4] A Secure Routing Protocol for Ad Hoc Networks, Bridget Dahill, Brian Neil, Elizabeth Royer, Clay Shields

[5] Routing Security in Ad Hoc Networks, Janne Lundberg, Helsinki University of Technology

[6] Security-Aware Ad-Hoc Routing for Wireless Networks, Seung Yi, Prasad Naldurg, Robin Kravets, Department of Computer Science.

[7] Mitigating Routing Misbehaviour in Ad Hoc Networks,

[8] Key Establishment in Ad Hoc Networks, Maarit Hietalahti, Helsinki University of Technology.

[9] Key Agreement in Dynamic Peer Groups, Michael Steiner, Gene Tsudik, Michael Waidner, IEE Computer Society.

[10] Mobile Ad Hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Consideration, S. Corson, J. Macker.

[11] The Resurrecting Duckling: Security Issues for Wireless Ad Hoc Mobile Networks. , F. Stajano and R. Anderson.

[12] A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks, E. M. Royer and C.K. Toh .

[13] The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks. J. Broch and D.B. Johnson

[14] Ad Hoc On-Demand Distance Vector Routing Protocol. C. E. Perkins and E. M. Royer.

[15] The Zone Routing Protocol (ZRP) for Ad Hoc Networks, Z. Haas and M. Pearlman.

AUTHORS

First Author – Manisha, Computer Science & Engineering B.S.A. Institute of Technology & Management , Faridabad, India, Email: prerna_sharma90@ymail.com

Second Author – Chanchal, Computer Science & Engineering B.S.A. Institute of Technology & Management , Faridabad, India, Email: chanchagarg.palwal@gmail.com

Third Author – Pawan Bhadana, Department of Computer Engineering, B.S.A. Institute of Technology & Management Faridabad, India

Fourth Author – Ritu Khurana , Department of Computer Engineering, B.S.A. Institute of Technology & Management Faridabad, India, Email: ritikakhurana11@gmail.com