Security Issues in the Ad-Hoc Network Environment

[1]Chinmaya Kumar Nayak, [2]Manoranjan Pradhan

[1]Assistant Professor, Department of Computer Science & Engineering, Gandhi Institute for Technological Advancement (GITA), Bhubaneswar, Odisha, India

[2]Ph. D, Professor and Head of the Department, Department of Computer Science & Engineering, Gandhi Institute for Technological Advancement (GITA), Bhubaneswar, Odisha, India

Abstract: ***Ad-hoc networks are an emerging area of mobile computing. There are various challenges that are faced in the Ad-hoc environment. These are mostly due to the resource poorness of these networks. They are usually set up in situations of emergency, for temporary operations or simply if there are no resources to set up elaborate networks. Ad-hoc networks therefore throw up new requirements and problems in all areas of networking. The solutions for conventional networks are usually not sufficient to provide efficient Ad-hoc operations. The wireless nature of communication and lack of any security infrastructure raise several security problems. In this paper we attempt to analyze the demands of Ad-hoc environment. We focus on Ad-hoc routing. 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.***

Keywords: Security problem, SAR, Message Authentication Code, Adhoc network.

1. Introduction

The contemporary routing protocols for Adhoc networks cope well with dynamically changing topology but are not designed to accommodate 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 malicious attackers who intend to bring down the network. External attackers - injects 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 [2][3].

Detection of compromised nodes through routing information is also difficult due to dynamic topology of Adhoc networks. Some properties of adhoc networks to facilitate secure routing can be used. Routing protocols for Adhoc 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 [4] [5].

2. Secure Routing In Ad-Hoc Networks

2.1 Problems associated with Ad-hoc routing

2.1.1 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. The nodes themselves are responsible for routing packets [6].

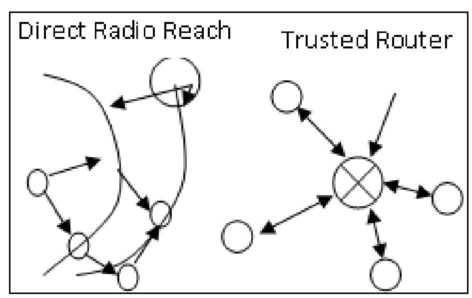

Figure 1: Routing in Ad-hoc networks and Routing in traditional networks using router

Each node relies on the other nodes to route packets for them. Mobile nodes in direct radio range of one another can communicate directly, but nodes that are too far apart to communicate directly must depend on the intermediate nodes to route messages for them.

2.1.2 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. As a result traditional routing protocols can no longer be used in such an environment. This mandates new routing protocols that can handle the dynamic topology by facilitating fresh route discoveries.

2.1.3 Problems associated with wirelesscommunication

As the communication is through wireless medium, it is possible for any intruder to tap the communication easily. Wireless channels offer poor protection and routing related control messages can be tampered. The wireless medium is susceptible to signal interference, jamming, eavesdropping and distortion [6]. An intruder can easily eavesdrop to know sensitive routing information or jam the signals to prevent propagation of routing information or worse interrupt messages and distort them to manipulate routes. Routing protocols should be well adopted to handle such problems.

2.1.4 Problems with existing Ad-hoc routing protocols

2.1.4.1 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 [7].

2.1.4.2 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.

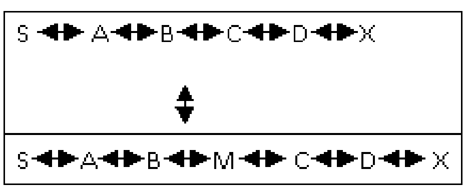

Figure 2: Forwarding packet by a malicious node

Misbehaving nodes can be a significant problem [8] [9]. Although the average loss in throughput due to misbehaving nodes is not too high, in the worst case it is very high.

2.1.4.3 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. For example, in the network illustrated in Figure 2, a malicious node M could keep traffic from reaching X by consistently advertising to B a shorter route to X than the route to X, which C is advertising.

3. Solutions to problems in Ad-hoc-routing

3.1 Concealing Network topology or structure

3.1.1 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 SAi 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 S As: SA1 → SA2 → …→SAN → R. The message is encapsulated N times using the public keys KSA1…KSAn as follows.

M' = KSA1 (SA2, (KSA2 (SA3 (… (KSAN(R, M))…))))

To deliver the packet, S sends it to the first security agent SA1 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.

3.1.2 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.

ZRP has some features that appear to make it somewhat less susceptible to routing attacks. Its hierarchical organization hides some of the routing information within the zones. ZRP provides some form of security against disclosing network topology by dividing routing into zones, which conceal the internal organization.

3.2 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.

3.2.1 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.

3.2.2 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.

3.2.3 Watchdog

The watchdog method detects misbehaving nodes. Figure3 illustrates how the watchdog works. Node A cannot transmit all the way to node C, but it can listen in on node B's traffic. Thus, when A transmits a packet for B to forward to C, A can often tell if B transmits the packet. If encryption is not performed separately for each link, which can be expensive, then A can also tell if B has tampered with the payload or the header.

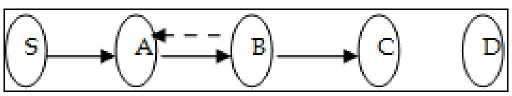

Figure 3: Operation of the watchdog.

We implement the watchdog by maintaining a buffer of recently sent packets and comparing each overheard packet with the packet in the buffer to see if there is a match. If so, the packet in the buffer is removed and forgotten by the watchdog, since it has been forwarded on. If the packet has remained in the buffer for longer than a certain timeout, the watchdog increments a failure tally for the node responsible for forwarding on the packet. If the tally exceeds a certain threshold bandwidth, it determines that the node is misbehaving and sends a message to the source notifying it of the misbehaving node.

Advantages: The watchdog mechanism can detect misbehaving nodes at forwarding level and not just the link level.
Weakness: It might not detect misbehaving nodes in presence of 1) ambiguous collusions 2) receiver collusions 3) limited transmission power 4) false misbehavior 5) collision 6) partial dropping.

3.2.4 Analysis of Watchdog's weaknesses

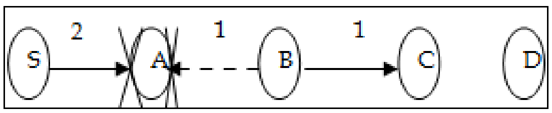

Figure 4: Ambiguous Collision

3.2.4.1 Ambiguous collision

The ambiguous collision problem prevents A from overhearing transmissions from B. As figure3.5 illustrates, a packet collision occur at A while it is listening for B to forward on a packet. A does not know if the collision was caused by forwarding on a packet as it should or if B never forwarded the packet and the collision was caused by other nodes in A's neighborhood. Because of this uncertainty, A should instead continue to watch B over a period of time.

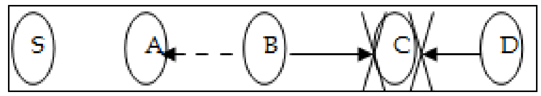

Figure 5: Receiver Collision.

3.2.4.2 Receiver collision

In the receiver collision problem, node A can only tell whether B sends the packet to C, but it cannot tell if C receives it. If a collision occurs at C when B first forwards the packet, A only sees B forwarding the packet and assumes that C successfully receives it. Thus, B could skip retransmitting the packet and evade detection [9][10].

3.2.4.3 False misbehavior

False misbehavior can occur when nodes falsely report other nodes as misbehaving. A malicious node could attempt to partition the network by claiming that some nodes following it in the path are misbehaving. For instance, node A could report that node B is not forwarding packets when in fact it is. This will cause S to mark B as misbehaving when A is the culprit. This behavior, however, will be detected. Since A is passing messages onto B (as verified by S), then any acknowledgements from D to S will go through A to S, and S will wonder why it receives replies from D when supposedly B dropped packets in the forward direction. In addition, if A drops acknowledgements to hide them from S, the node B will detect this misbehavior and will report it to D.

3.2.4.4 Limited transmission power

Another problem is that a misbehaving node that can control its transmission power can circumvent the watchdog. A node could limit its transmission power such that the signal is strong enough to be overheard by the previous node but too weak to be received by the true recipient.

3.2.4.5 Multiple colluding nodes

Multiple nodes in collusion can mount a more sophisticated attack. For example, B and C from figure3.4 could collude to cause mischief. In this case, B forwards a packet to C but does not report to A when C drops the packet. Because of its limitation, it may be necessary to disallow two consecutive untrusted nodes in a routing path.

3.2.4.6 Partial dropping

A node can circumvent the watchdog by dropping packets at a lower rate than the watchdog's configured minimum misbehavior threshold. Although the watchdog will not detect this node as misbehaving, this node is forced to forward at the threshold bandwidth. In this way the watchdog serves to enforce this minimum bandwidth. For the watchdog to work properly it must know where a packet should be in two hops.

3.3 Pathrater

Just like the watchdog, the pathrater is run by each node. It combines the knowledge of misbehaving nodes with link reliability data to pick. Each node maintains a rating for every other node it knows about in the network. It calculates a path metric by averaging the node ratings in the path. We choose this metric because it gives a comparison of the overall reliability of different paths and allows pathrater to emulate the shortest length path algorithm when no reliability information ahs been collected, as explained below. If there are multiple paths to the same destination, we choose the path with the highest metric. Since the pathrater depends on knowing the exact path a packet has traversed, it must be implemented on top of a source routing protocol.

The pathrater assigns ratings to nodes according to the following algorithm. When anode in the network becomes known to the pathrater (through route discovery), the pathrater assigns it a "neutral" rating of 0.5. A node always rates itself with a 1.0. This ensures that when calculating path rates, if all other nodes are neutral nodes (rather than suspected misbehaving nodes); the pathrater picks the shortest length path. The pathrater increments the ratings of nodes on all actively used paths by 0.01 at periodic intervals of 200 ms. An actively used path is one on which the node has sent a packet within the previous rate increment interval. The maximum value a neutral node can attain is 0.8. We decrement a node's rating by 0.05 when we detect a link break during packet forwarding and the node becomes unreachable. The lower bound rating of a "neutral" node is 0.0. The pathrater does not modify the ratings of nodes that are not currently in active use.

We assign special highly negative value, -100 in the simulations, to nodes suspected of misbehaving by the watchdog mechanism. When the pathrater calculates the path metric, negative path values indicate the existence of one or more suspected misbehaving nodes in the path. If a node is marked as misbehaving due to a temporary malfunction or incorrect accusation it would be preferable if it were not permanently excluded from routing. Therefore nodes that have negative ratings should have their ratings slowly increased or set back to a non-negative value after a long timeout.

3.3.1 Performance Throughput and Overhead

The watchdog and pathrater mechanism with DSR algorithm improves throughput by 27% while increasing the overhead from 12% to 24%. But this overhead is due to the way DSR operates to maintain routes. The watchdog itself adds very little overhead. Although the overhead is significant, these extensions still improve net throughput. In networks with moderate mobility throughput improves by 17% while overhead transmission increases from 9% to 17%.

3.4 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) [12]. A node initiating route discovery sets the sought security level for the route i.e. the required minimal trust level for nodes participating in the query/ reply propagation[13],[14]. Nodes at each trust level share symmetric encryption keys. Intermediate nodes of different levels cannot decrypt in-transit routing packets or determine whether the required security attributes can be satisfied and drop them. Only the nodes with the correct key can read the header and forward the packet. So if a packet has reached the destination, it must have been propagated by nodes at the same level, since only they can decrypt the packet, see its header and forward it.

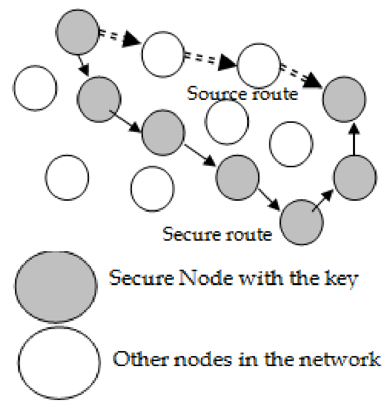

Figure 6: Forwarding packet by secure route

3.5 Implementation

SAR can extend any routing protocol. Here we see how to extend AODV and call it SAODV. Most of AODV's original behavior such as on-demand discovery using flooding, reverse path maintenance and forward path setup via Route Request and Reply (RREP) messages is retained.

The RREQ (Route REQuest) and the RREP (Route REPly) packets formats are modified to carry additional security information. The RREQ packet has an additional field called RQ_SEC_REQIREMENT that indicates the required security level for the route the sender wishes to discover. This could be a bit vector.. An intermediate node at the required trust level, updates the RREQ packet by updating another new field, RQ_SEC_GUARANTEE field. The RQ_SEC_GUARANTEE field contains the minimum security offered in the route. This can be achieved if each intermediate node at the required trust level performs an 'AND' operation with RQ_SEC_GUARANTEE field it receives and puts the updated value back in to the RQ_SEC_GUARANTEE field before forwarding the packet.

Finally the packet reaches the destination if a route exists. In the RREP packet one additional field is also added. When an RREQ successfully traverses the network to the sender, the RQ_SEC_GUARANTEE represents the minimum security level in the entire path from source to destination. So the destination copies this from the RREQ to the RREP, into a new field called RP_SEC_GUARANTEE field. The sender can use this value to determine the security level on the whole path, since the sender can find routes which offer more security than asked for, with which he can make informed decisions.

Drawbacks: A lot of encryption overhead, since each intermediate node has to performs it.

3.6 Secure Routing Protocol

A Security Association (SA) exists between the source node (S) and destination node (T).One way of establishing this SA is negotiating a shared secret key by the knowledge of the public key of the other end. The existence of the SA is justified, because the end hosts choose a secure communication scheme and consequently should be able to authenticate each other. The SA would be established by any of group key exchange schemes [9] [11]. However the exists of SAs with any of the intermediate nodes is unnecessary. It is required that the end nodes be able to use non-volatile memory to maintain state information regarding relayed queries, so that previously seen route requests are discarded. It is also expected that a one to one mapping exists between MAC and IP addresses exists. Finally the broadcast nature of the radio channels requires that each transmission is received by all neighbors, which are assumed to operate in promiscuous mode (i.e. able to overhear all transmissions from nodes within the range of their transceiver).

3.6.1 Working

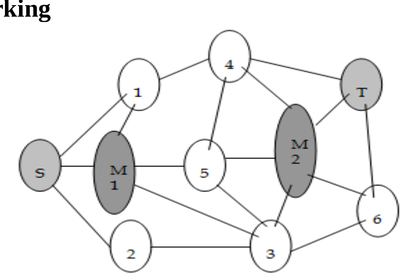

Figure 7: Secure Routing Network

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 KST) 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 KST i.e. MAC = h(S, T, rnd#, sq#, KST). 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.

4. Advantages

Computing the MAC is not computationally expensive. Message integrity is preserved. If confidentiality of data is required we could encrypt the pay load with the shared key KST. Different attacks on routing and how they are countered

Let M1, M2 be two malicious intermediate nodes.

We denote the query request as a list {QST; n1, n2… nk}. QST denotes the SRP header for a query searching for T and initiated by S.

ni, i not = {1 ,k} are the IP addresses of the intermediate nodes and n1= S, nk= T.

Similarly, a route reply is denoted as {RST; n1, n2, …. nk}

Case 1:
When M receives {QST; S} it tries to mislead S by generating {RST; S, M1, T} i.e. it fakes that destination T is its neighbor. This is possible in a regular routing protocol, but not here, since only T can generate the MAC which is verified by S.

Case 2:
If M1 discards request packets that it receives, it narrows the topology view of S. But at the same time it practically removes itself from S's view. Thus it cannot inflict harm to data flows originating from S, and route chosen by S would not include M1.

Case 3:
When M1 receives {RST; S, 1, M1, S, 4, T} it tampers with its contents and relays {RST; S, 1, M, Y, T}. Y being any sequence of nodes, S readily discards the reply due to the integrity protection provided by MAC.

Case 4:
When M2 receives {QST; S, 2, 3} it corrupts the accumulated route and relays

{QST; S, X, 3, M2} to its neighbors, where X is a false IP address. This request arrives at T, which constructs the reply and routes it over {T, M2, 3, X, S} towards S. but when node 3 receives the reply it cannot forward it any further since X is not its neighbor and the reply is dropped.

Case 5:
If M1 replays route requests to consume network resources, they will be discarded by intermediate nodes, since they maintain a list of query identifiers seen in the past. The query identifier is a random number, so that it is not guessable by the malicious node.

Case 6:
If M1 attempts to forward {QST; S, M*} i.e. it spoofs its IP address. Consequently S would accept {RST; S, M*, 1, 4, T} as a route. But the connectivity information conveyed by such a reply is correct. However, in practice, neighbor discovery that maintain information on the binding of the MAC and IP address can strengthen the protocol. Packets would be discarded when relayed by same data link interface i.e. same MAC address with more than one different IP address.

3.7 Attacks on SRP Protocol

Tunneling

If 2 nodes collude during the 2 phases (request and reply) of a single route discovery, then the protocol could be attacked. e.g.: if M1 received a route request, it can tunnel it to M2 i.e. discover a route to M2 and send the request encapsulated in a data packet. Then M2 broadcasts a request with the route segment between M1 and M2 falsified { QST; S, M1, Z, M2}. T receives the request and constructs a reply which is routed one {T, M2, Z, M1, S}. M2 receives the reply and tunnels it back to M1, which then returns it to S. As a result the connectivity information is only partially correct.

5. Replay

If M1 rewrites the RND# with some other random number, its neighbors think that it is a genuine packet and keep forwarding it, thus wasting their resources. Only when the packet reaches the destination can this misuse be detected using the MAC.

6. Conclusion

We have presented an overview of the existing security scenario in the Ad-Hoc network environment. Key management, Ad-hoc routing aspects of wireless Ad-hoc networks was 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 [1]. But the flexibility, ease and speed with which these networks can be set up implies they will gain wider application [14] [15]. This leaves Ad-hoc networks wide open for research to meet these demanding application.

References

[1] Yongguang Zhang, Wenke Lee, Yi-An Huang"Intrusion Detection in Wireless Ad-hoc Networks", Wireless Networks 9 (5), 545-556,2003
[2] N.Asokan, Philip Ginzboorg, "Key Agreement in Adhoc Networks, Preprint submitted to Elsevier preprint,3 Frebuary 2003
[3] L. Zhou, Z.J. Haas, Cornell Univ., "Securing ad hoc networks," IEEE Network, Volume: 13 , Page(s): 24-30, ISSN: 0890-8044. Nov/Dec 1999
[4] B Dahill, BN Levine, E Royer, C Shields "A Secure Routing Protocol for Ad Hoc Networks" Network Protocols, 2002. Proceedings. 10th IEEE International Conference on 12-15 Nov. 2002
[5] Janne Lundberg, Helsinki University of Technology,Routing Security in Ad Hoc Networks, Tik-110.501 Seminar on Network Security, HUT TML 2000
[6] Seung Yi, Prasad Naldurg, Robin Kravets, Security-Aware Ad-Hoc Routing for Wireless Networks, Proceeding MobiHoc '01 Proceedings of the 2nd ACM international symposium on Mobile ad hoc networking & computing, Pages 299-302, ACM New York, NY, USA ©2001
[7] S Marti, TJ Giuli, K Lai, M Baker, "Mitigating Routing Misbehaviour in Ad Hoc Networks",International Conference on Mobile Computing and Networking: Proceedings,2000
[8] Maarit Hietalahti,Key Establishment in Ad Hoc Networks, Electronic Notes in Theoretical Computer Science, Elsevier,2008
[9] M Steiner, G Tsudik, MWaidner Key Agreement in Dynamic Peer Groups" Parallel and Distributed Systems, IEEE Transactions on 11 (8), 769-780, 2000.
[10] S. Corson, J. Macker,"Mobile Ad Hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Consideration", MANET Performance Issues January 1999
[11] RJ Anderson, MG Kuhn "Information hiding-a survey",FAP Petitcolas, Proceedings of the IEEE 87 (7), 1062-1078,1999
[12] E. M. Royer and C.K. Toh." Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks",Personal Communications, IEEE 6 (2), 46 -55A, 1999
[13] DB Johnson, DA Maltz," The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks",KluwerInternational Series in Engineering and Computer Science, 153-179,1996
[14] Perkins, Charles E., and Elizabeth Royer. "Ad-Hoc On-Demand Distance Vector Routing." WMCSA'99. Second IEEE Workshop on, 1999
[15] ZJ Haas, MR Pearlman," The performance of query control schemes for the zone routing protocol", IEEE/ACM Transactions on Networking (TON) 9 (4), 427-438,2001

Author Profile

Chinmaya Kumar Nayak is an Assistant Professor in the Department of Computer Science & Engineering, Gandhi Institute for Technological Advancement (GITA), Bhubaneswar, Odisha, India. He is an author of the book "Data Structure Using C". He published many papers in national seminars and international journals. His research area includes image processing, adhoc networks etc.

International Journal of Scientific Engineering and Research (IJSER)
www.ijser.in
ISSN (Online): 2347-3878
Volume 1 Issue 1, September 2013

Manoranjan Pradhan holds a Ph. D Degree in Computer Science. He is presently working as a professor and Head of the Department of Computer Science & Engineering, Gandhi Institute for Technological Advancement (GITA), Bhubaneswar, Odisha, India. He has 14 years of teaching experience. He has published many papers in national and international journals. His research interests include Computer Security, Intrusion Detection and Soft Computing.