Mobile Ad Hoc

Anil Dahiya[1]
[1]Department of Computer Science &Engineering,
Ganga Institute of Technology and Management,
Kablana, Jhajjar, Haryana, India

Abstract: **Mobile Ad hoc have been highly venerable to attacks due to the dynamic nature of its network infrastructure. Among these attacks ,routing attacks have received considerable attention since it could cause the most devastating damage to Mamet even though there exist several intrusion response techniques to mitigate such critical attacks ,exiting solutions typically attempt to isolate malicious nodes based on binary or naïve fuzzy response decision . however ,binary responses may result in the unexpected network partition ,causing additional damages to the network infrastructure and naïve fuzzy responses could lead to uncertainty in countering routing attacks in Mamet .In this paper we propose a risk, aware response mechanism to systematically cope with the identified routing attacks. our risk aware approach is based on an extended dempster _shafer mathematically theory of evidence introducing a notion of importance factors .**

1. INTRODUCTION

A mobile ad hoc network (MANET) is a collection of mobile devices that can communicate with each other without the use of a predefined infrastructure or centralized administration. In addition to freedom of mobility, a MANET can be constructed quickly at a low cost, as it does not rely on existing network infrastructure. Due to this flexibility, a MANET is attractive for applications such as disaster relief, emergency operations, military service, maritime communications, vehicle networks, casual meetings, campus networks, robot networks, and so on.

Unlike the conventional network, a MANET is characterized by having a dynamic, continuously changing network topology due to mobility of nodes [1]. This feature makes it difficult to perform routing in a MANET compared with a conventional wired network.

Network: Another characteristic of a MANET is its resource constraints, that is, limited bandwidth and limited battery power. This characteristic makes routing in a MANET an even more challenging task. Therefore, early work in MANET research focused on providing routing service with minimum cost in terms of bandwidth and battery power.

Currently, several efficient routing protocols have been proposed. These protocols can be classified into two categories: reactive routing protocols and proactive routing protocols. In reactive routing protocols, such as the Ad hoc Infrastructure-less: Central servers, specialized hardware, and fixed infrastructures are necessarily absent. The lack of infrastructure precludes the deployment of hierarchical host relationships; instead, nodes uphold egalitarian relationships. That is, they assume contributory On Demand Distance Vector (AODV) protocol [2], nodes find routes only when required. In proactive routing protocols, such as the Optimized Link State Routing (OLSR) protocol [3], nodes obtain routes by periodic exchange of topology information. Most of these routing protocols rely on cooperation between nodes due to the lack of a centralized administration and assume that all nodes are trustworthy and well-behaved.

Fig.1 Example of MANET

The survey has been done on the current state of the art of attacks on the network layer, that is, routing attacks such as link spoofing, wormhole attacks, and colluding misrelay attacks, as well as countermeasures in a MANET. Then, an overview of countermeasures for each attack and an overview of routing protocols in a MANET.

II. MANET'S FEATURES AND THEIR IMPACT ON SECURITY

The features of MANETs make them more vulnerable to attacks and misbehavior than traditional networks, and impose the security solution to be different from those used in other networks. These features are:

Infrastructure-less: Central servers, specialized hardware, and fixed infrastructures are necessarily absent. The lack of infrastructure precludes the deployment of hierarchical host relationships; instead, nodes uphold egalitarian relationships. That is, they assume contributory collaborative roles in the network rather than ones of dependence. i.e any

collaborative roles in the network rather than ones of dependence. i.e any security solution should rely on cooperative scheme instead of centralized one.

- Wireless links use: The use of wireless links renders a wireless ad hoc network susceptible to attacks. Unlike wired networks where an adversary must gain physical access to the network wires or pass through several lines of defense at firewalls and gateways, attacks on a wireless ad-hoc network can come from all directions and target at any node. Hence, a wireless ad hoc network will not have a clear line of defense, and every node must be prepared to threats. Moreover, since the channel is widely accessible, the MAC protocols used in ad hoc networks, such IEEE802.11, rely on trusted cooperation in a neighborhood to ensure channel access, which presents vulnerability.
- Multi-hop: Because the lack of central routers and gateways, hosts are themselves routers, then packets follow multi-hop routes and pass through different mobile nodes before arriving to the destination. Because of the possible untrustworthy of such nodes, this feature presents a serious vulnerability.

III. TYPES OF ATTACKS

It includes any action that intentionally aims to cause any damage to the network; it can be divided according to their origins or their nature.

Origin based classification splits attacks up into two categories; external and internal, whereas, nature based classification splits them up into passive attacks and active attacks

External attacks: This category Includes attacks launched by a node that do not belong to the logical network, or is not allowed to access to it. Such a node penetrates the network area to launch its attack .Internal attacks: This category includes attacks launched by an internal compromised node; It is a more several kind of threat to the network since the proposed defense toward external attacks is ineffective against compromised and internal malicious nodes.

Passive attacks: A passive attack is a continuous collection of information; this information would be used later when launching an active attack. That means the attacker eavesdrops packets and analyzes them to pick up required information. The security attribute that must be provided here is information confidentiality.

Active attacks: Include almost all the other attacks launched by actively interacting with victims, like sleep deprivation torture that aims the batteries charges, hijacking, in which the attacker takes control of a communication between two entities and masquerades as one of them, jamming, that causes channel unavailability, attacks against routing protocols, etc... Most of these attacks result in a denial of service (DoS) that is degradation or a complete halt in communication between nodes.

IV. ROUTING PROTOCOLS IN MANETS

Efficient routing of packets is a primary manet Challenge. Manets use multihop rather than single-hop routing to deliver packets to their destination. The goal of routing in a MANET is to discover the most recent topology of a continuously changing network to find a correct route to a specific node. At network layer, routing protocols are used to find route for transmission of packets. Routing is the most fundamental research issue in ad hoc networking. Mobile Ad Hoc Network presents unique advanced challenges, including the design of protocols for mobility management, effective routing, data transport, security, power management and Quality of Service provisioning.

Pro-Active Protocols: They attempt to maintain consistent up-to-date routing information from each node to every other node in the network. These protocols require each node to maintain one or more tables to store routing information, and any changes in network topology need to be reflected by propagating updates throughout the network in order to maintain a consistent network view.

Dynamic Destination-Sequenced Distance-Vector routing algorithm[6].Based on Bellman-Ford routing algorithm:- Every mobile station maintains and uses for routing packets ,a routing table, listing all available destinations, the number of hops to reach the destination and the sequence number assigned by the destination. The sequence number distinguishes old routes from new ones. Stations periodically and on significant changes transmit their routing tables to their neighbors.

Destination-Sequenced Distance-Vector Routing (DSDV) is a table-driven routing scheme for ad hoc mobile networks based on the Bellman-Ford algorithm. It was developed by C. Perkins and P.Bhagwat in 1994. The main contribution of the algorithm was to solve the routing loop problem. Each entry in the routing table contains a sequence number, the sequence numbers are generally even if a link is present; else, an odd number is used. The number is generated by the destination, and the emitter needs to send out the next update with this number. Routing information is distributed between nodes by sending *full dumps* infrequently and smaller incremental updates more frequently.

Global State Routing.: Based on link state routing but avoids flooding of routing messages. Each node maintains a Neighbor list, a Topology table, a Next hop table and a Distance table. The routing messages are generated on a link change and the node updates its topology table if the sequence number of the message is newer than the number stored in the table.

The link-state protocol is performed by every *switching node* in the network (i.e. nodes that are prepared to forward packets; in the Internet, these are called routers). The basic concept of link-state routing is that every node constructs a *map* of the connectivity to the network, in the form of a graph, showing which nodes are connected to which other nodes. Each node then independently calculates the next best logical *path* from it to every possible destination in the network. The collection of best paths will then form the node's routing table.

This contrasts with distance-vector routing protocols, which work by having each node share its routing table

with its neighbors. In a link-state protocol the only information passed between nodes is connectivity related.

The routing messages are generated on a link change as in link state protocols. On receiving a routing message, the node updates its Topology table if the sequence number of the message is newer than the sequence number stored in the table. After this the node reconstructs its routing table and broadcasts the information to its neighbor.

Fisheye State Routing: In FSR each update message contains information about closest nodes frequently and farther nodes as required i.e. detail and accuracy of information decreases as the distance from node increases.

Fisheye State Routing (FSR) is an improvement of GSR. The large size of update messages in GSR wastes a considerable amount of network bandwidth. In FSR, each update message does not contain information about all nodes. Instead, it exchanges information about closer nodes more frequently than it does about farther nodes thus reducing the update message size.

V. RE-ACTIVE PROTOCOLS

Reactive Routing protocols are based on finding routes between two nodes , when it is required. This is different from traditional Proactive Routing Protocols in which nodes periodically sends messages to each other in order to maintain routes. Only Reactive Protocols are considered in this article, as they are extensively studied and used in MANETs. Among many Reactive Routing Protocols, only three of them are described below as they are mostly studied.

Ad hoc On Demand Distance Vector Routing: This algorithm enables dynamic, self-starting multi hop routing between nodes. This method does not require nodes to maintain routes to destinations that are out of active communication. It is 1st protocol to do multicasting as well as unicasting. Sequence no. is used by routers.A reverse path is followed by it.

To find a path to the destination, the source broadcasts a route request packet. The neighbors in turn broadcast the packet to their neighbors till it reaches an intermediate node that has a recent route information about the destination or till it reaches the destination (Figure 3a). A node discards a route request packet that it has already seen. The route request packet uses sequence numbers to ensure that the routes are loop free and to make sure that if the intermediate nodes reply to route requests, they reply with the latest information only.

When a node forwards a route request packet to its neighbors, it also records in its tables the node from which the first copy of the request came. This information is used to construct the reverse path for the route reply packet. AODV uses only symmetric links because the route reply packet follows the reverse path of route request packet. As the route reply packet traverses back to the source (Figure 3b), the nodes along the path enter the forward route into their tables.

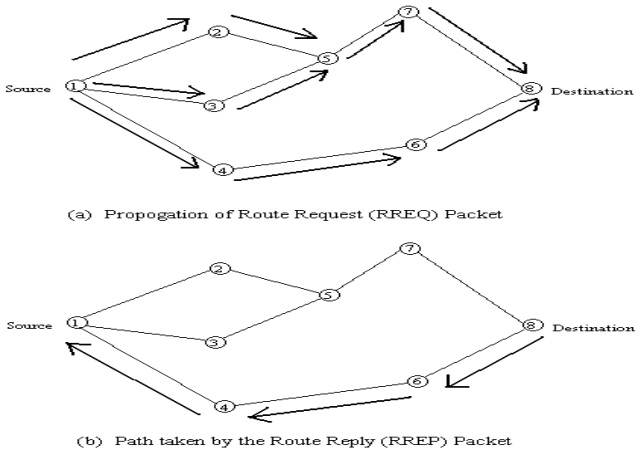

Fig.2.Aodv Routing Protocol

Temporary-Ordered routing Algorithm: It is an adaptive routing protocol for multihop networks and has following features.

- Distributed execution ,
- Loop free and multipath routing,
- Reactive or Proactive root establishment.
- Localization of algorithmic reactions to topological changes.
- based on the concept of link reversal
- It finds multiple routes from a source node to a destination node

Zone Routing Protocol It combines the advantages of the proactive (for nodes within the zone) and reactive (for nodes outside) approaches

Hybrid Approach: A recently proposed hybrid approach6 captures the advantages of on-demand and optimized linkstate routing for wireless sensor networks.

Zone Routing Protocol: It combines the advantages of the proactive (for nodes within the zone) and reactive (for nodes outside) approaches

VI. ROUTING ATTACKS AGAINST MANET PROTOCOLS

MANETs are much more vulnerable to attack than wired network. This is because of the following reasons:

- Open Medium - Eavesdropping is easier than in wired network.
- Dynamically Changing Network Topology – Mobile Nodes comes and goes from the network, thereby allowing any malicious node to join the network without being detected.
- Cooperative Algorithms - The routing algorithm of MANETs requires mutual trust between nodes which violates the principles of Network Security.
- Lack of Centralized Monitoring - Absence of any centralized infrastructure prohibits any monitoring agent in the system.

- Lack of Clear Line of Defense - The only use of I line of defense - attack prevention may not succeed. In addition to prevention, we need II line of defense - detection and response.

Security Attacks on Protocol Stacks:

LAYERS	ATTACKS
Multilayer Attack	DOS, Impersonation, Reply, Man in the middle
Application Layer	Repudiation, Data corruption
Transport Layer	Session hijacking, SYN flooding
Network Layer	Wormhole , Black whole, Flooding, Resource consumption ,Location disclosure
Data link Layer	Traffic analysis, Monitoring, Disruption MAC,WEP weakness
Physical layer	Jamming, interception, Eavesdropping

Fig.3 Table of layers & related attacks

VII. FLOODING ATTACK

SOLUTIONS TO THE FLOODING ATTACK: In this approach, each node monitors and calculates the rate of its neighbors' RREQ [11]. If the RREQ rate of any neighbor exceeds the predefined threshold, the node records the ID of this neighbor in a blacklist. Then, the node drops any future RREQs from nodes that are listed in the blacklist. One limitation of this approach is that it cannot prevent against the flooding attack in which the flooding rate is below the threshold. Another drawback of this approach is that if a malicious node impersonates the ID of a legitimate node and broadcasts a large number of RREQs, other nodes might put the ID of this legitimate node on the blacklist by mistake.

Another adaptive technique is to mitigate the effect of a flooding attack in the AODV protocol. This technique is based on statistical analysis to detect malicious RREQ floods and avoid the forwarding of such packets. In this approach, each node monitors the RREQ it receives and maintains a count of RREQs received from each sender during the preset time period. The RREQs from a sender whose RREQ rate is above the threshold will be dropped without forwarding. Unlike the method proposed, where the threshold is set to be fixed, this approach determines the threshold based on a statistical analysis of RREQs. The key advantage of this approach is that it can reduce the impact of the attack for varying flooding rates.

VIII. BLACKHOLE ATTACK

In a blackhole 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 (including a fake destination sequence number that is fabricated to be equal or higher than the one contained in the RREQ) to the source node, claiming that it has a sufficiently fresh route to the destination node. This causes the source node to select the route that passes through the attacker. Therefore, all traffic will be routed through the attacker, and therefore, the attacker can misuse or discard the traffic. Figure shows an example of a blackhole attack, where attacker A sends a fake RREP to the source node S, claiming that it has a sufficiently fresher route than other nodes. Since the attacker's advertised sequence number is higher than other nodes' sequence numbers, the source node S will choose the route that passes through node A.

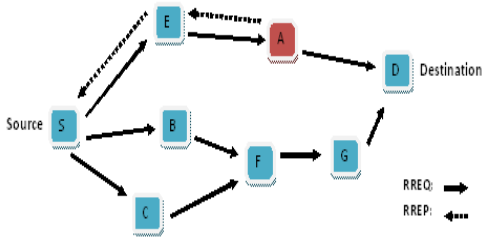

Fig.4 Blackhole Attack

SOLUTIONS TO BLACKHOLE ATTACK: The route confirmation request (CREQ) and route confirmation reply (CREP) are used to avoid the blackhole attack. In this approach, the intermediate node not only sends RREPs to the source node but also sends CREQs to its next-hop node toward the destination node. After receiving a CREQ, the next-hop node looks up its cache for a route to the destination. If it has the route, it sends the CREP to the source. Upon receiving the CREP, the source node can confirm the validity of the path by comparing the path in RREP and the one in CREP. If both are matched, the source node judges that the route is correct. One drawback of this approach is that it cannot avoid the blackhole attack in which two consecutive nodes work in collusion, that is, when the next-hop node is a colluding attacker sending CREPs that support the incorrect path.

Another solution requires a source node to wait until a RREP packet arrives from more than two nodes. Upon receiving multiple RREPs, the source node checks whether there is a shared hop or not. If there is, the source node judges that the route is safe. The main drawback of this solution is that it introduces time delay, because it must wait until multiple RREPs arrive.

IX. LINK WITHHOLDING ATTACK

In this attack, a malicious node ignores the requirement to advertise the link of specific nodes or a group of nodes, which can result in link loss to these nodes. This type of attack is particularly serious in the OLSR protocol.

SOLUTIONS TO WITHHOLDING ATTACK: By withholding a TC message in OLSR, a malicious node can isolate a specific node and prevent it from receiving data packets from other nodes. After analyzing and evaluating

the impact of this kind of attack in detail, a detection technique is proposed based on observation of both a TC message and a HELLO message generated by the MPR nodes. If a node does not hear a TC message from its MPR node regularly but hears only a HELLO message, a node judges that the MPR node is suspicious and can avoid the attack by selecting one or more extra MPR nodes.

The main drawback of this approach is that it cannot detect the attack that is launched by two colluding consecutive nodes, where the first attacker pretends to advertise a TC message, but the second attacker drops this TC message.

X LINK SPOOFING ATTACK

In a link spoofing attack, a malicious node advertises fake links with non-neighbors to disrupt routing operations. For example, in the OLSR protocol, an attacker can advertise a fake link with a target's two-hop neighbors. This causes the target node to select the malicious node to be its MPR. As an MPR node, a malicious node can then manipulate data or routing traffic, for example, modifying or dropping the routing traffic or performing other types of DoS attacks.

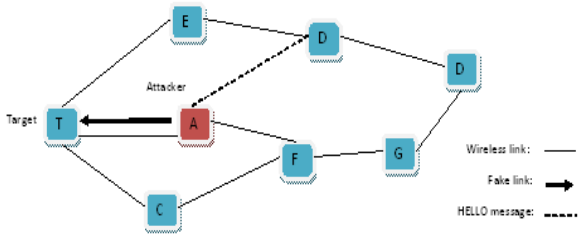

Fig. 5 Link Spoofing Attack

SOLUTIONS TO LINK SPOOFING ATTACK: To detect a link spoofing attack, a location information-based detection method is used by using cryptography with a GPS and a time stamp. This approach requires each node to advertise its position obtained by the GPS and the time stamp to enable each node to obtain the location information of the other nodes. This approach detects the link spoofing by calculating the distance between two nodes that claim to be neighbors and checking the likelihood that the link is based on a maximum transmission range. The main drawback of this approach is that it might not work in a situation where all MANET nodes are not equipped with a GPS. Furthermore, attackers can still advertise false information and make it hard for other nodes to detect the attack[19].

Another technique to detect the link spoofing attack is by adding two-hop information to a HELLO message. In particular, the proposed solution requires each node to advertise its two-hop neighbors to enable each node to learn complete topology up to three hops and detect the inconsistency when the link spoofing attack is launched. The main advantage of this approach is that it can detect the link spoofing attack without using special hardware such as a GPS or requiring time synchronization. One limitation of this approach is that it might not detect link spoofing with nodes further away than three hops.

X. REPLAY ATTACK

In a MANET, topology frequently changes due to node mobility. This means that current network topology might not exist in the future. In a replay attack [20], a node records another node's valid control messages and resends them later. This causes other nodes to record their routing table with stale routes. Replay attack can be misused to impersonate a specific node or simply to disturb the routing operation in a MANET.

SOLUTIONS TO REPLAY ATTACK: A solution to protect a MANET from a replay attack is by using a time stamp with the use of an asymmetric key. This solution prevents the replay attack by comparing the current time and time stamp contained in the received message. If the time stamp is too far from the current time, the message is judged to be suspicious and is rejected. Although this solution works well against the replay attack, it is still vulnerable to a wormhole attack where two colluding attackers use a high speed network to replay messages in a far-away location with almost no delay.

XI. WORMHOLE ATTACK

A wormhole attack 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. The seriousness of this attack is that it can be launched against all communications that provide authenticity and confidentiality. Figure 3 shows an example of the wormhole attack against a reactive routing protocol. In the figure, we assume that nodes *A*1 and *A*2 are two colluding attackers and that node S is the target to be attacked. During the attack, when source node S broadcasts an RREQ to find a route to a destination node D, its neighbors C and E forward the RREQ as usual. However, node *A*1, which received the RREQ, forwarded by node C, records and tunnels the RREQ to its colluding partner *A*2. Then, node *A*2 rebroadcasts this RREQ to its neighbor H. Since this RREQ passed through a high-speed channel, this RREQ will reach node D first. Therefore, node D will choose route D-H-C-S to unicast an RREP to the source node S and ignore the same RREQ that arrived later. As a result, S will select route S-CH- D that indeed passed through *A*1 and *A*2 to send its data.

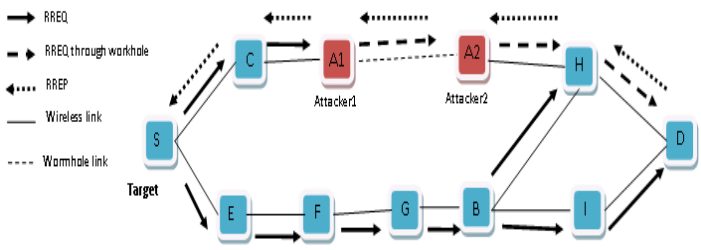

Fig. 6 Wormhole Attack

SOLUTIONS TO WORMHOLE ATTACK: Packet leashes are proposed to detect and defend against the wormhole attack. In particular, the authors proposed two types of leashes: temporal leashes and geographical leashes. For the temporal leash approach, each node computes the packet expiration time, *te*, based on the speed of light *c* and includes the expiration time, *te*, in its packet to prevent the packet from traveling further than a specific distance, *L*. The receiver of the packet checks whether or not the packet expires by comparing its current time and the *te* in the packet. The authors also proposed TIK, which is used to authenticate the expiration time that can otherwise be modified by the malicious node. The main drawback of the temporal leash is that it requires all nodes to have tightly synchronized clocks.

For the geographical leash, each node must know its own position and have loosely synchronized clocks. In this approach, a sender of a packet includes its current position and the sending time. Therefore, a receiver can judge neighbor relations by computing distance between itself and the sender of the packet. The advantage of geographic leashes over temporal leashes is that the time synchronization need not to be highly tight.

Another approach is based on protection against a wormhole attack in the OLSR protocol. This approach is based on location information and requires the deployment of ijhnnja public key infrastructure and timestamp synchronization between all nodes. In this approach, a sender of a HELLO message includes its current position and current time in its HELLO message. Upon receiving a HELLO message from a neighbor, a node calculates the distance between itself and its neighbor, based on a position provided in the HELLO message. If the distance is more than the maximum transmission range, the node judges that the HELLO message is highly suspicious and might be tunneled by a wormhole attack.

XII. COLLUDING MISRELAY ATTACK

In this attack, multiple attackers work in collusion to modify or drop routing packets to disrupt routing operation in a MANET. This attack is difficult to detect by using the conventional methods such as *watchdog* and *pathrater* [23,24]. Figure shows an example of this attack. Consider the case where node *A*1 forwards routing packets for node T. In the figure, the first attacker *A*1 forwards routing packets as usual to avoid being detected by node T. However, the second attacker A2 drops or modifies these routing packets. In the authors discuss this type of attack in OLSR protocol and show that a pair of malicious nodes can disrupt up to 100 percent of data packets in the OLSR MANET.

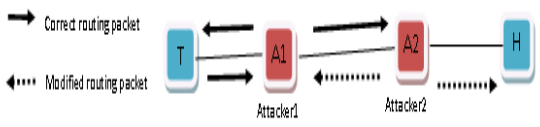

Fig. 7 Colluding Attack

SOLUTIONS TO COLLUDING ATTACK: A conventional acknowledgment-based approach might detect this type of attack in a MANET, especially in a proactive MANET, but because routing packets destined to all nodes in the network require all nodes to return an ACK, this could lead to a large overhead, which is considered to be inefficient.

To detect an attack in which multiple malicious nodes attempt to drop packets is by requiring each node to tune their transmission power when they forward packets. As an example, the author studies the case where two colluding attackers drop packets. The proposed solution requires each node to increase its transmission power twice to detect such an attack. However, this approach might not detect the attack in which three colluding attackers work in collusion. In general, the main drawback of this approach is that even if we require each node to increase transmission power to be *K* times, we still cannot detect the attack in which $K + 1$ attackers work in collusion to drop packets. Therefore, further work must be done to counter against this type of attack efficiently.

XIII. ADVANTAGE & DISADVANTAGE

The following are the advantages of MANETs:

- They provide access to information and services regardless of geographic position.
- These networks can be set up at any place and time.

Some of the disadvantages of MANETs are:

- Limited resources.
- Limited physical security.
- Intrinsic mutual trust vulnerable to attacks.
- Lack of authorization facilities.
- Volatile network topology makes it hard to detect malicious nodes.
- Security protocols for wired networks cannot work for ad hoc networks.

XIV. FUTURE WORK

Future research should be focused not only on improving the effectiveness of the security schemes but also on minimizing the cost to make them suitable for a MANET environment. Furthermore, each proposed solution can work only with a specific attack and is still vulnerable to unexpected attacks. The Security research area is still open as many of the provided solutions are designed keeping a limited size scenario and limited kind of attacks and vulnerabilities. Therefore, MANET researchers should also focus on exploring, as well as preventing all possible attacks to make a MANET a secure and reliable network.

REFERENCES

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

[2] C. Perkins, E Royer,"Ad Hoc On-Demand Distance Vector Routing", 2nd IEEE Wksp. Mobile Comp. Sys.and Apps., 1999.

[3] D. Johnson, D. Maltz, "Dynamic Source Routing in Ad Hoc Wireless Networks", Mobile Computing, Imielinski and H. Korth, Ed., Kluwer, 1996. 3] M.S. Corson, J.P. Maker, and J.H. Cernicione, Internet-based Mobile Ad Hoc Networking, IEEE Internet Computing, pages 63–70, July-August 1999.

[4] Amitabh Mishra, Ketan M. Nadkarni, "Security in Wireless Ad Hoc Networks", in Book The Handbook of Ad Hoc Wireless Networks (Chapter 30), CRC Press LLC, 2003.

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