Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 5, May 2013, pg.360 – 367

RESEARCH ARTICLE

ROUTING ATTACKS IN MOBILE AD HOC NETWORKS

P. Narendra Reddy[1], CH. Vishnuvardhan[2], V. Ramesh[3]

[1]Computer science, JNTU-A/ Sree Vidyanikethan Engineering College, Tirupati, India

[2]Computer science, JNTU-A/ Sree Vidyanikethan Engineering College, Tirupati, India

[3]Computer science, Research scholar Sathyabama University, Chennai, Tamilnadu, India

[1] g.narendra111@gmail.com; [2] vishnuvardhan.gdr@gmail.com; [3] v2ramesh634@yahoo.co.in

Abstract— Mobile ad hoc networks (MANETs) are a set of mobile nodes which are self-configuring and connected by wireless links automatically as per the defined routing protocol. These nodes communicate with each other by exchange of packets, which for those nodes not in wireless range goes hop by hop. Unique characteristics, such as dynamic network topology, limited bandwidth, and limited power, nodes running on battery routing in a MANET is a particularly challenging task compared to a conventional network. MANET research has focused on developing an efficient hybrid routing mechanism in such a highly dynamic mobile nodes in network. At present, several efficient routing protocols have been proposed for MANET. However, in the presence of malicious nodes, the networks are vulnerable is possible to various kinds of attacks. In particular, we examine routing attacks, such as link spoofing and colluding miss relay attacks, as well as countermeasures against such attacks in existing MANET protocols.

Key Terms: - Mobile Ad hoc Networks; Routing Protocols; Attacks; Flooding; Blackhole

I. INTRODUCTION

Basic diagram showing ad-hoc network Mobile Ad hoc Network (MANET) is a set of mobile devices (nodes), which over a shared wireless medium communicate with each other without the presence of a predefined infrastructure or a central authority 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. The chief characteristics and challenges of the MANETs can be classified as follows:

1) Cooperation:

If the source node and destination node are out of range with each other than the communication between them takes place with the cooperation of other nodes such that a valid and optimum chain of mutually connected nodes are formed. This is known as multi hop communication. Each node is to act as a host as well as a router simultaneously.

2) *Dynamism of Topology:*

The nodes of MANET are frequently, randomly and unpredictably mobile within the network. The nodes are may leave or join of the network at any point of time, so that nodes mobility and the complexity of routing is very high. Such mobility entails that the topology of the network as well as the connectivity between the hosts is unpredictable.

3) Lack of fixed infrastructure:

The absence of a fixed or central infrastructure is a key feature of MANETs. That mobile node are not stable, this eliminates the possibility to establish a centralized authority to control the network characteristics. Traditional techniques of network management and security are scarcely not applicable to MANETs.

4) Resource constraints:

MANETs are a set of mobile devices which are of low or limited power capacity (it run's on battery), computational capacity (mobility), memory, bandwidth etc. by default in Routing a secure and reliable communication between nodes.

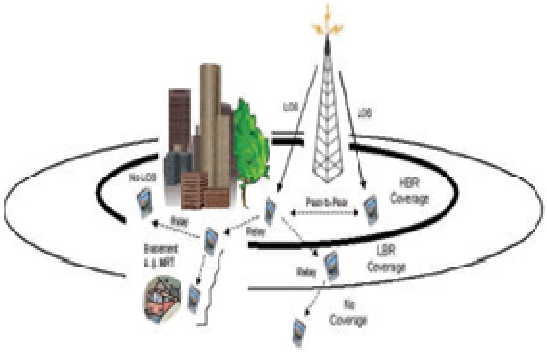

Fig-1: Mobile Ad hoc Networks

The MANET is attractive for applications such as disaster relief, military service, robot networks, emergency operations, maritime communications, casual meetings, campus networks, vehicle networks, and so on. Unlike conventional network, a MANET is characterized by having a high dynamic nature, 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. Several efficient routing protocols have been proposed. These protocols can be classified into three categories:

a) Reactive routing protocols
b) Proactive routing protocols
c) Hybrid routing protocols

In reactive routing protocols, such as the Ad hoc 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. A malicious node can launch routing attacks to disrupt routing operations or denial-of-service (DoS) attacks [4] to deny services to legitimate nodes.

Hybrid routing protocols uses a mix of both proactive and reactive routing protocols. This hybrid protocols can be used to find a balance between the table-driven and on demand protocols. The idea behind hybrid routing protocols is to use both routing protocols, proactive mechanisms in some areas of the network at certain times and reactive routing for the rest of the network. The proactive operations are limited to a small domain in order to reduce the control delays and overheads. The reactive routing protocols are used for locating the mobile nodes outside domain, as this is more bandwidth-efficient in a constantly changing mobile network. Examples of hybrid routing protocols: Ad Hoc Routing Protocol (CEDAR) [14], Zone Routing Protocol (ZRP) [15], and Zone Based Hierarchical Link State Routing Protocol (ZHLS).

Most of the previous work focused mainly on providing preventive schemes to protect the routing protocol in a MANET. In general, the limitation of these approaches is that they introduce a heavy traffic load to exchange, which is very expensive in terms of the bandwidth-constraint for MANET nodes with limited and limited computational capabilities. In [9], the survey attacks and their countermeasures in mobile ad hoc network for TCP/IP (five layers) For attacks against the network layer(TCP/IP)authors survey countermeasures for impersonation routing attacks in MENETs, modification attacks, wormhole attacks, and blackhole attacks. However, new attacks and countermeasures against a network layer attack in TCP/IP, the art of attacks on the network layer, routing attacks such as link spoofing, wormhole attacks, and colluding miss relay attacks, as well as countermeasures in a MANET.

II. ROUTING ATTACKS IN MANET PROTOCOLS

1) FLOODING ATTACK

The aim of the flooding attack [11] is to exhaust the network resources: bandwidth and to consume a node's resources, such as battery power and computational or to disrupt the routing operation to cause severe

degradation in network, Flood attacks occur when a network or service becomes so weighed down with packets initiating incomplete connection requests that it can no longer process genuine connection requests

2) BLACKHOLE ATTACK

In a black hole routing attack, a malicious (attacker) node sends fake routing information to the other nodes, claiming that it has an optimum route to destination and causes other good nodes to route data packets through the malicious one. 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, malicious node claiming that it has a sufficiently fresh route to the destination node. This causes the source node to select a route that passes through the (malicious) attacker, all traffic will be routed through the attacker, and therefore, attacker node can misuse or discard the traffic, in MENETs.

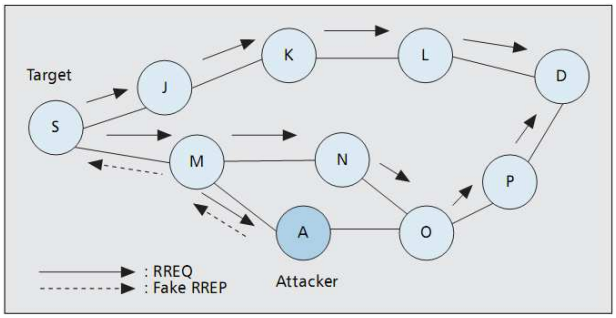

Fig2: Example of Blackhole Attack

3) 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.

4) LINK SPOOFING ATTACK

In a spoofing attack, the malicious node advertises fake link with non-neighbors to disrupt routing, in the OLSR protocol, an attacker can advertise a fake link with the target's two-hop neighbors.

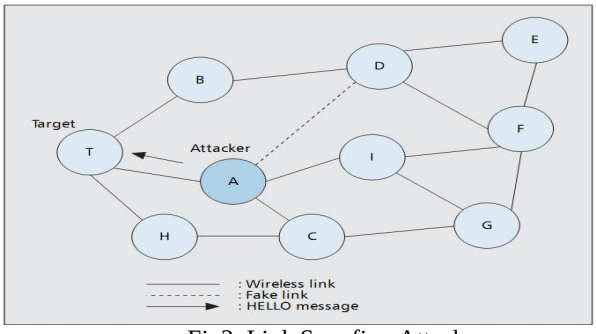

Fig3: Link Spoofing Attack

A malicious node can manipulate data or routing traffic: dropping or modifying the routing traffic or performing other types of DoS attacks in this data.

5) REPLAY ATTACK

In a MANET, topology frequently changes due to mobility of nodes. This means that current network topology might not exist for after some time. In this attack, a node records another node's valid control messages and it's resends to destination later. This attack 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 operations in a MANET.

6) WORMHOLE ATTACK

In this attack [9] one of the most sophisticated and severe side attacks in MANETs, a pair of colluding attackers record packets at one location after that the attacker will replay them at another location using a private high speed network to destination node The seriousness of this attack that it can be launched against the all communications that provide authenticity and confidentiality.

7) COLLUDING MISRELAY ATTACK

In colluding misrelay attack, multiple attackers work at a time in collusion to modify or drop routing packets to disrupt routing to destination in a MANET. This attack is very difficult to detect by using the old methods such as watchdog and path rater [10].

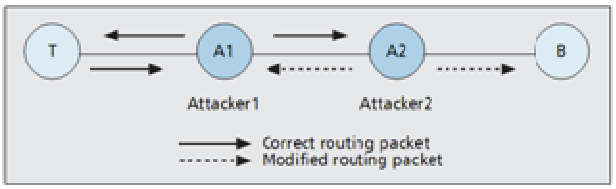

Fig4: Colluding Misrelay Attack

8) *NODE ISOLATION ATTACK*

The authors in this work have introduced the attack against an OLSR protocol. As implied by name, the main goal of this attack is to isolate the given node from communicating with other nodes with in the network. The idea of this attack is attacker(s) prevent link information of a specific node or a group of nodes from being spread to into the network. Other nodes who could not receive link information of these target nodes will not be able to build a route to these target nodes, hence will not be able to send data packet's to these nodes.

9) ROUTING TABLE POISONING ATTACK

In this attack the different routing protocols maintain routing tables which hold information regarding routes of the destination or neighbor nodes network. The attacker node generates and sends false traffic, or mutates legitimate messages from other nodes, to create false entries in the routing tables of the participating nodes. Another possibility is to inject the RREQ packet with a high sequence number, all other legitimate RREQ packets with lower sequence numbers to be deleted. Routing table poisoning attacker can result in selection of nonoptimal routes, creation of routing loops in network, bottlenecks and even partitioning certain parts of the network.

10) WORMHOLE ATTACK

The wormhole attack involves cooperation between the two attacking nodes [14]. One attacker captures the routing traffic at one of the point in network and tunnels it to another point of the network that shares a private high speed communication link between the attackers, and then selectively injects tunnel traffic to back the network. The two colluding attacker can potentially distort the topology and establish routes under the control over the wormhole link.

11) LOCATION DISCLOSURE ATTACK

In this attack, the privacy requirements of a node are compromised. Through the use of traffic analysis technique or with simpler probing and monitoring approaches an attacker is able to discover a location of the node, and the structure of the network.

12) WORMHOLE ATTACK

The wormhole attack involves the cooperation between the two attacking nodes. One of the attacker node captures routing traffic or data at one point of the network, tunnels into another point in the network that shares a private high speed communication link between the attackers, and then selectively injects tunnel traffic back into the network. The two colluding the attacker can potentially distort the topology and establish routes under the control over the wormhole link.

13) LOCATION DISCLOSURE ATTACK

In this attack, the privacy requirements of the node are compromised in the network. Through the use of traffic analysis techniques or with simpler probing and monitoring approaches an attacker is able to discover the location of a node, and it discovery the structure of the network also by using this attack.

14) *RUSHING ATTACKS*

The attacker node initiates a Route Discovery packet for the target node. If the RREQ for this Discovery forwarded by the attacker are the first to reach each neighbor of the destination or target, then any route discovered by the Route Discovery will include a hop through the attacker. When the neighbor of the target receives the false REQUEST from the attacker node, that node forwards that REQUEST to another nodes, and

sometimes will not forward any further REQUESTs from this Route Discovery, because of the node capability. When non attacking RREQs arrive later at these nodes, they will discard those legitimate RREQs from the original node. As a result, the initiator will be unable to discover any usable routes (i.e., routes that do not include the attacker) containing at least two hops (three nodes).

13) BLACKMAIL

The attack unpleasant due to lack of authenticity and it grants provision for any another nodes to corrupt, Valid information to nodes usually keep information of perceived attacker nodes in a blacklist. This type of attack is relevant against routing protocols that use mechanisms for the identification of malicious nodes and propagate messages that try to blacklist. An attacker may equipment such reporting messages and tells other nodes in the network to add that node to their blacklists and isolate valid nodes from the network.

14) *THE INVISIBLE NODE ATTACK*

We have defined the invisible node or attacker, that node proved it to be different from the existing attacks for example man in the middle and masquerading, and established its uniqueness. That have defined it as Inn any routing protocol that depends on identification of any functionality that used by the node, any node that effectively participates in the protocols without revealing its identity is an invisible node and the action and protocol impact is termed an INA. The effects of INA on different routing protocols, they have shown it to be an unsolvable attack so far.

III. COUNTERMEASURES AGAINST ATTACKS

In this section, we discuss solutions that are proposed to counter against routing attacks described in the previous section.

1) SOLUTIONS TO THE FLOODING ATTACK

The authors proposed [11] a simple mechanism to prevent the flooding attack in the AODV Protocol. In this method, each node monitors and calculates the rate of neighbors' RREQ for each node in the network. If any node RREQ rate of any neighbor node exceeds the predefined value or threshold, that node records the all the ID of this neighbor into the blacklist. The node drops any RREQs from nodes that are also listed in the blacklist. If one limitation of this method is that it cannot prevent against the flooding attack in which the flooding rate is below the threshold. The main limitation of this approach is that if a malicious node impersonates the ID of a valid node and broadcasts large number of RREQs for destination, other nodes might put the ID of this legitimate node on the blacklist by mistake .In [12], the authors proposed an adaptive technique to mitigate the effect of a flooding attack in the AODV protocol. Technique is based on statistical analysis to detect malicious RREQ floods and avoid the forwarding of such type of packets. Similar, each node monitors the RREQ it receives and maintains a count of RREQs received from each sender during some period of time. The RREQs from a sender whose RREQ rate is above the threshold will be dropped without forwarding. This approach determines the threshold based on the statistical analysis value of RREQs for each node. The main advantage of this approach is that it can reduce the impact of the attacker for varying flooding rates in the network.

2) SOLUTIONS TO THE BLACKHOLE ATTACK

In [13], the authors introduce the route confirmation request (CREQ) and route confirmation reply (CREP) to avoid the blackhole attack. In this Technique, the intermediate node not only sends RREPs to the source node but also sends CREQs to its next-hop node toward the destination node. If the node 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. Based on receiving the CREP, the source node will confirm the validity of the path by comparing the path in RREP and the one in CREP. If the both are matched, the source node judges that the route is correct to source to destination. One drawback of this Technique is that it cannot eliminate the black hole attack in which two consecutive nodes work in collusion in the network, Hence when the next-hop node is a colluding attacker sending CREPs that support the incorrect path to destination node .The another authors proposed a solution that requires a source node to wait until a RREP packet arrives from more than two nodes. Based on the receiving multiple RREPs, the source will checks the whether there is a shared hop or not in the route, the source node judges that the route is safe. The drawback of this method is that it introduces time delay, because it must wait until for multiple RREPs arrive for particular node, analyzed the blackhole attack and showed that a malicious node must increase the destination sequence number sufficiently to convince the source node that the route provided is sufficiently enough. Based on this analysis, propose a statistical based anomaly detection approach to detect the blackhole attack, based on differences between the destination sequence numbers of the received RREPs The key advantage of this approach is that I can detect the attack at low cost without introducing extra

routing traffic, and it does not modification of the existing protocol. However, false positives are the one of drawback of this approach due to the nature of anomaly detection.

3) SOLUTIONS TO THE MESSAGE WITHHOLDING ATTACK

In [16], the authors show that by withholding a TC message in OLSR protocol, an attacker node can isolate specific node and prevent it from receiving data or control packets from other nodes. After analyzing and evaluating the impact of this kind of attack in detail, the authors proposed a detection technique based on observation of both a TC message and a HELLO message generated by the MPR nodes. If any node does not hear a TC message from any node its MPR node regularly but hears only a HELLO message from a node, judges that the MPR node is illegal and can avoid the attack by selecting one or more extra MPR nodes in the network. Similarly, in [15], another authors proposed an intrusion detection system to detect TC link and message withholding in the OLSR protocol, each node observes whether an MPR node generates a TC message regularly or not. In case an MPR node generates a TC message regularly, node checks whether or not the TC message actually contains itself to detect the attack. The drawback of this is method that they cannot detect the attack that is launched by two colluding consecutive nodes, where the first attacker node pretends the advertise a TC message, but the second attacker node drops this TC message.

4) SOLUTIONS TO THE LINK SPOOFING ATTACK

To detect a link spoofing attack, the author of [15] proposed a location information-based detection method by using cryptography with a GPS and a time stamp. Require search 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. The method 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 drawback of this method is that it might not work in a situation where all MANET nodes are not equipped with a GPS, attackers can still advertise wrong information and make it hard for other nodes to detect the attack. In [5], the authors show that a malicious node that advertises fake links with a target's two-hop neighbors can successfully make the target choose it as the only MPR. Through simulations, the authors show that link spoofing can have a devastating impact on the target node. Technique to detect the link spoofing attack by adding two-hop information to a HELLO message to node. 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 method is that it can detect link spoofing attack without using special hardware such as a GPS or requiring time synchronization. One drawback of this approach is that it might not detect link spoofing with nodes further away than three hops.

5) SOLUTIONS TO THE REPLAY ATTACK

In [10], the authors proposed a solution for to replay attack protect a MANETs, the replay attack 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. In case 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 their play 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. This attack will be discussed in the next subsection.

6) SOLUTIONS TO THE WORMHOLE ATTACK

In [10], packet leashes are to detect and defend against the wormhole attack. the two types of leashes: For the temporal leash method each node computes the packet expiration time t_e based on the speed of light c and includes the expiration time t_e 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 t_e in the packet, which is used to authenticate the expiration of time that can used otherwise modified by the malicious node. The limitation of the temporal leash is that it requires all nodes to have closely synchronized clocks for nodes. For the geographical leash, each node must know its own position and have loosely synchronized clocks, a sender of a packet includes its current position and the sending time, a receiver can judge neighbor relations by computing distance between itself and the sender of the packet. The main advantage of this method is geographic leashes over temporal leashes is that the time synchronization needs not to be highly tight in [15], protection against a wormhole attack in the OLSR protocol. Another method is based on location information and requires the deployment of a public key infrastructure and time-stamp synchronization between all nodes that is similar to the geographic; 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. In [12], statistical analysis of multipath (SAM), which is an method to

find out the wormhole attack by using multipath routing. This method determines the attack by calculating the relative frequency of each link that appears in all of the obtained routes from one route discovery, a link that has the highest relative frequency is identified as the wormhole link. The advantage of this method is that it introduces limited overhead when applied in multipath routing. However, that might not be work in a non-multipath routing protocol, such as a pure AODV protocol.

7) SOLUTIONS TO A COLLUDING MISRELAY ATTACK

A conventional acknowledgment-based method might detect this type of attack in a MANET, the especially in a proactive MANET, but in routing packets destined to all nodes in the network require all nodes to return an ACK, this traffic or could lead to a large overhead on network, which is considered to be in inefficient. In [6], a method to detect an attack in which multiple malicious nodes attempt to drop packets by requiring each node to tune their transmission power when they forward packets. As an example, the studies the case where two colluding attackers drop packets. The solution requires each node to increase its transmission power twice to detect such an attack. However, this method might not detect the attack in which three colluding attackers work in collusion. In general, the limitation of this method is that even if we require each node to increase transmission power to be K times, still cannot detect the attack in which $K + 1$ attackers work in collusion to drop packets, work must be done to counter against this type of attack efficiently.

8) SOLUTION TO NODE ISOLATION ATTACK:

The malicious node can isolate a specific node and prevent it from receiving data packets from other nodes by withholding a TC message in OLSR protocol, the method a detection technique based on observation of both a TC message and a HELLO message generated by the MPR nodes is proposed, a node judges that the MPR node is suspicious and can avoid the attack by selecting one or more extra MPR nodes. Another IDS that detects TC link and message withholding in the OLSR protocol, nodes is set to observe whether a MPR node generates a TC message regularly or not. If a MPR node generates a TC message regularly, the node checks whether or not the TC message actually contains itself to detect the attack. The drawback of these approaches is that they cannot detect the attack if it that is launched by two colluding next hop nodes, where the first attacker pretends to advertise a TC message, but the second attacker drops this TC message.

9) SOLUTIONS TO THE RUSHING ATTACK:

In [35] Hu et al. have proposed a set of generic mechanisms that together defend against the rushing attacks secure neighbor detection, secure route delegation process, and Randomized RREQ packet's forwarding to every node . A secure neighbor detection allows each neighbor to verify that the other is within a given maximum transmission range or not. Once a node A determines that node B is a neighbor it signs a Route Delegation message to that node, allowing node B to forward the RREQ. When node B determines that node A is within the allowable range, it signs an Accept Delegation message from the source node. The Randomized selection of RREQ message to be forwarding which replaces traditional duplicate suppression in on demand route discovery.

10) *SOLUTION TO THE SNARE ATTACK:*

In Lin et al. have defined the snare attack and he proposed ASRPAKE (An Anonymous Secure Routing Protocol with Authenticated Key Exchange for Wireless Ad Hoc Networks) algorithm, Decoy node deployment to mitigate this snare attack. The proposed anonymous secure routing protocol consists of five phases: route discovery phase, key pre-distribution phase, neighborhood discovery phase, route reverse phase, and the data forwarding phase in this method the anonymity of the VIN can further be enhanced using no. of decoy nodes which allow the communication to be routed to the VIN only after verifying the authenticity of the source node in the network. The features of this method are achievable end-to end anonymity and security the integration of the Authenticated key exchange operations into the routing algorithm.

11) TRUST BASED SECURITY SOLUTIONS

Another active area of research in Mobile Ad Hoc and Sensor Network security in general is the Trust Based Security Solutions, have identified the role of Trust in MANETs, When the network entity establishes trust in other network entities, it can predict the future behaviors of others and diagnose their security properties for each node. Trust helps in Assistance indecision making to improve security and robustness of network, Adaptation to risk leading to flexible security solutions, Misbehavior detection and Quantitative assessment of system-level security properties.

IV. CONCLUSION AND FUTURE WORK

A MANET is an emerging technology that has been attracting tremendous attention from researchers. Because these networks can be deployed quickly without relying on a predefined infrastructure, they can be applied in various situations ranging from emergency operations and disaster relief to military service and task forces, obviously, providing security in such scenarios is critical. The main weaknesses of a MANET are that it is resource constrained, for example, a MANET has limited bandwidth, battery power, and computational power, and it lacks a reliable centralized administration. Therefore, existing security schemes for wire networks cannot be applied directly to a MANET, which makes a MANET much more vulnerable to security attacks. In this article, we reviewed the current state of- the-art of routing attacks and countermeasures in a MANET. For countermeasures, we identified their advantages as well as their drawbacks. Our studies showed that although many solutions have been proposed, they still are not perfect in terms of tradeoffs between effectiveness and efficiency. For example, some solutions that rely on cryptography and key management seem promising but they are high expensive for resource-constrained MANETs. Although some solutions work well in the presence of one attacker node, they might not be applicable in the presence of multiple colluding attackers. Some solutions may require some special hardware such as a GPS or a modification to the existing protocol.

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. 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] Ajay Jangra, NitinGoel, Priyanka, Komal, Security Aspects in Mobile Ad Hoc Network (MANETs): A Big Picture‖, International Journal of Electronics Engineering, 2(1), 2010, pp. 189-196.

[2] C.Siva Ram Murthy & B.S Manoj, M obile Ad Hoc Networks- Architectures & Protocols‖, Pearson Education,New Delhi, 2004.

[3] Behrouz A Forouzan, Data Communications and Networking‖, Special Indian Forth Edition, 2006

[4] SinemColeri ,Ergen, ZigBee IEEE 802.15.4‖September 10, 2004 . LAN-MAN Standards Committee of the IEEE Computer Society, Wireless LAN medium access control (MAC) and physical layer (PHY) specification, IEEE, New York, NY, USA, IEEE Std802.11-1997 edition,1997 .
Wireless Communication, pp. 35 – 54, ISBN 9781420045474. An Introduction to Wi-Fi 019-0170 • 090409-B USA 2007-2008.

[5] Caroline Gabriel, WiMax, ARCchart ltd., London EC2A 1LN.

[6] B R Sujatha, M V Satyanarayana, Improved Network Connectivity in MANETs‖, International Journal of Computer Networks & Communications (IJCNC), Vol.1, No.3, October 2009.

[7] Ajay Jangra, SunitaBeniwal, Anil Garg, C o-existence behavior study of Bluetooth & Wi-Fi for 2.4 GHz ISM band‖2006.

[8] J. U. Duncombe, "Infrared navigation—Part I: An assessment of feasibility," IEEE Trans. Electron Devices, vol. ED-11, pp. 34-39, Jan. 1959.

[9] C. Y. Lin, M. Wu, J. A. Bloom, I. J. Cox, and M. Miller, "Rotation, scale, and translation resilient public watermarking for images," IEEE Trans. Image Process., vol. 10, no. 5, pp. 767-782, May 2001.

[10] Y-C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," Proc.MobiCom '02, Atlanta, GA, Sept. 23–28, 2002.

[11] M. G. Zapata and N. Asokan, "Securing Ad-Hoc RoutingProtocols," Proc. 2002 ACM Wksp. Wireless Sec., Sept.2002, pp. 1–10.

[12] B. Wu et al., "A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks," Wireless/Mobile Network Security, Springer, vol. 17, 2006.

[13] S. Marti et al., "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," 6th MobiCom, Boston, MA, Aug. 2000.

[14] P. Yi et al., "A New Routing Attack in Mobile Ad Hoc Networks," Int'l. J. Info. Tech., vol. 11, no. 2, 2005.

[15] S. Desilva, and R. V. Boppana, "Mitigating Malicious Control Packet Floods in Ad Hoc Networks," Proc. IEEE Wireless Commun. and Networking Conf., New Orleans, LA, 2005.
S. Lee, B. Han, and M. Shin, "Robust Routing in Wire-less Ad Hoc Networks," 2002 Int'l. Conf. Parallel Pro-cessing Wksps., Vancouver, Canada, Aug. 18–21, 2002.

