ISSN 2229-5518

Privacy Anxiety and Challenges in Mobile Ad Hoc Wireless Networks and its Solution

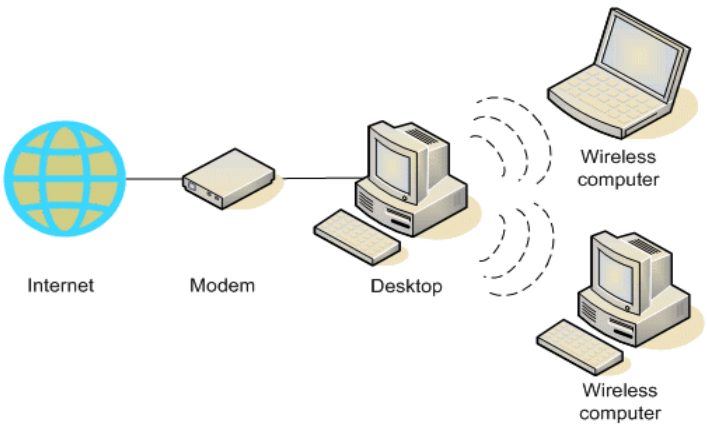
Krishan Kant Lavania, G. L. Saini, Kothari Rooshabh H., Yagnik Harshraj A.

Abstract— Mobile Ad hoc networks are recent wireless networking model for cellular phone hosts. Ad hoc networks do not rely on any stable infrastructure because they are independent. As an alternative, to remain network connected hosts rely on each other. It signifies complex distributed systems that encompass wireless mobile nodes. These nodes can freely and dynamically self-organize into uninformed and provisional, "ad-hoc" network topologies. This topology allows citizens to effortlessly interconnect in areas where no pre-existing communication infrastructure. In this paper, we talk about security issues, challenges and their solutions in the mobile ad hoc network. There are numerous security threats that disturb the development of mobile ad hoc network because of the exposed nature of the mobile ad hoc network. We have first studied the prime vulnerabilities in the mobile ad hoc networks, which have made our work much easier to endure from attacks than the usual wired network. The security criteria of the mobile ad hoc network and the main attack types that exist are explained in this paper. As a final point we analyzed the recent security solutions for the mobile ad hoc network [1].

Index Terms— Minimum 7 keywords are mandatory, Keywords should closely reflect the topic and should optimally characterize the paper. Use about four key words or phrases in alphabetical order, separated by commas.

1 Introduction

An ad hoc network is a set of wireless mobile nodes that forms a momentary network with no central organization. In this situation, it may be essential for one mobile node to enroll other hosts for forwarding a packet from source node to its destination node due to the restricted transmission range of wireless network interfaces. Each mobile node operates as a router for forwarding packets for many other mobile nodes in the network that may not have direct communication range of each other. To discover multihop paths through network each node participates with other node in an ad hoc routing protocol. This proposal of Mobile ad hoc network is also called infrastructure less networking [2].



Ad hoc networks have a unique set of challenges and problems, although mobile ad hoc networks have numerous advantages over the traditional wired networks. For example the supply constraints on nodes in ad hoc networks bound the cryptographic procedures that are used for secure messages. That's why it is legally responsible to fix attacks ranging from passive masquerade to active masquerade. Secondly, mobile nodes with no enough protection are easy to conciliation. An attacker can listen, modify and attempt to cover-up all the traffic on the wireless communication channel as one of the valid node in the network. Thirdly, in provisions of security solution and for the vigorously changing topology static configuration is not sufficient. In conclusion, deficiency of cooperation and guarded ability is common in wireless MANET. In universal, due to its fundamental uniqueness of the wireless MANET, it is vulnerable.

A MANET Example

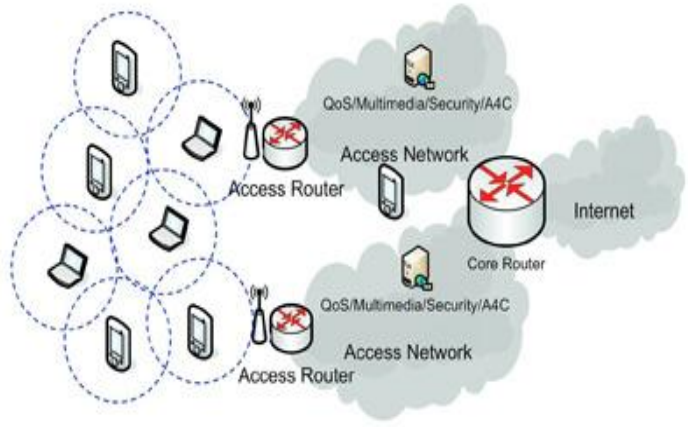


Fig. Shows MANET Example

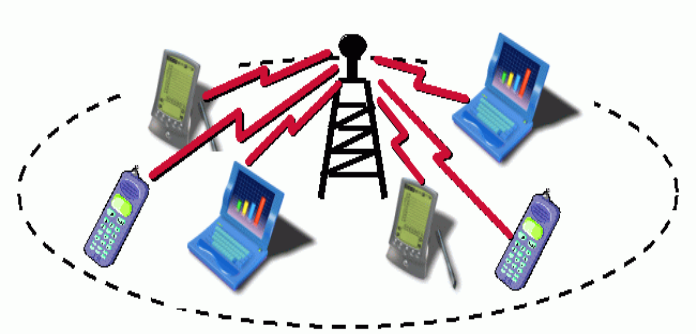
2 MANET Concept

A mobile ad hoc network is a set of wireless nodes that can dynamically be set up at everyplace and anytime without using any pre-existing network infrastructure. It is an self-sufficient system in which mobile hosts connected by wireless links. They are free to move randomly and often operate as routers at the same time. The traffic types in ad hoc

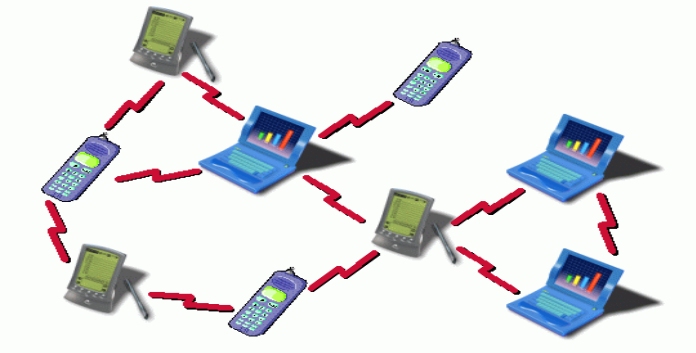
networks are relatively different from an infrastructure wireless network, including [3]:

(1) Peer-to-Peer
(2) Remote-to-Remote
(3) Dynamic Traffic

1) Peer-to-Peer- It means communication that is between two nodes in network which are within one hop. Network traffic is usually steady.
2) Remote-to-Remote-It means communication that is between two nodes away from a single hop but which retain a secure route between them. The traffic is related to standard network traffic.
3) Dynamic Traffic- Dynamic traffic usually occurs when nodes are dynamic and moving around. Their routes must be reconstructed. This results in a poor connectivity.



(a) Infrastructure-based wireless network



Features of MANETs

1) With minimum infrastructure support
2) Multi-hop
3) Self-organizing
4) Self-managing
5) All of the nodes in network are mobile
6) Varied network topology
7) Wireless network
8) Node is a host
9) Node is a router
10) Power restriction
11) Balance Variant
12) Heterogeneous network

3 Security Attacks in Mobile Ad Hoc Wireless Networks

There are two types of security attacks:-
(a)Basic security attacks in Mobile Ad Hoc Wireless Networks
(b)Various other types of possible security attacks in Mobile Ad Hoc Wireless Networks

[a] Basic security attacks in Mobile Ad Hoc Wireless Networks

They are classified into two types:
– Passive

- A mean node pay no attention to necessary operations that are supposed to be Accomplished by it (For e.g.: partial routing information hiding), or attempting to Retrieve important and secure information.

– Active

- Important Information is routed through direct or indirect channel to the network in a active attack, and thus the nodes and some operation of network may be Harmed. For E.g.: spoofing, modification and fabrication.

[b] Other Types of Possible security attacks in Mobile Ad Hoc Wireless Networks

Masquerade

✓ Nodes may be able to send false routing information to other node.
✓ Masquerading is also possible as some other trusted node.
✓ Here a mean node uses the routing protocol to promote itself as having the shortest path to the node whose packets node wants to intercept this attack is known as "The Black Hole attack"[4].

Denial of Service (DoS)

✓ The intruder attempts to utilize batteries of other nodes by requesting routes.
✓ The intruder also keeps busy other nodes by forwarding unnecessary packets.

Handling misbehaviors

Nodes that are selfish results in Routing-forwarding misbehaviors.

- ✓ Due to the malicious or selfish node network functioning is damaged.
- ✓ A selfish node misbehaves because this node wants to save battery life for their own communication. This can be done by not executing the packet forwarding or simply not participating in the routing protocol.
- ✓ To contradict misbehavior of selfish node, cooperation can be enforced.

- ✓ By reputation mechanism and watchdog we can detect selfish nodes misbehavior.
- ✓ Neighborhood monitoring is a technique by which watchdog identifies misbehaving selfish nodes.
- ✓ Based on the information collected by the watchdog, the reputation system maintains a value for each node that represents the node's reputation.
- ✓ The reputation mechanism allows nodes to segregate misbehaving nodes by not serving their requests.
- ✓ A different approach of countering misbehavior is to encourage nodes to collaborate and stay away from selfish behavior through an incentive system.

Routing Attacks

- ✓ Generating fake Route Error to interrupt a functioning route.
- ✓ To spoof route message impersonating another node.
- ✓ To misrepresent the topology marketing a forged route metric.
- ✓ To Deceive others it Suppress Route Error.
- ✓ To suppress other justifiable route messages it Send a route message with wrong sequence number.
- ✓ Flooding Route ascertain terribly as a Denial of Service attack.
- ✓ To introduce a false route it modifying a Route Reply message.

4 MANET Challenges

The characteristics of MANET bring in various challenges that must be considered
With awareness before a broad commercial deployment can be expected. These consist of [5]:

a) Internetworking. Harmonious mobility management is a challenge in mobile device due to coexistence of routing protocols.

b) Security and Reliability. An ad hoc network has its particular security problems due to e.g. nasty neighbor relaying packets in spite of accumulation to the frequent vulnerabilities of wireless connection. Additionally wireless link features commence also reliability problems, because of the restricted wireless transmission range, data transmission errors, the broadcast nature of the wireless medium, and mobility-induced packet losses.

c) Quality of Service (QoS). It will be a challenge on providing various qualities of service levels in a persistently varying environment. It makes complicated to propose fixed guarantees on the services offered to a device due to intrinsic stochastic feature of communications quality in a MANET.

d) Routing. The concern of routing packets between any pair of nodes becomes a challenging task since the topology of the network is frequently changing. Due to the random movement of nodes within the network the multicast tree is no longer static so multicast routing is another challenge. Routing is becoming more complex and challenging because routes between nodes may potentially contain multiple hops, than the single hop communication.

e) Power Consumption. Power-aware routing and Maintenance of power must be taken into consideration. For lean power consumption the communication-related functions should be optimized for most of the light-weight mobile terminals [6].

5 Mobile Ad Hoc Networks Security Solutions

The mobile ad hoc networks become insecure due to various vulnerabilities. As a result, we require discovering various security solutions to the mobile ad hoc network. We analyzed some security schemes that can be helpful to protect the mobile ad hoc network from nasty behaviors.

Security Criteria

Before we analyzed the solutions that can assist secure the mobile ad hoc network, we have to find out on basis of which criteria we can judge that a mobile ad hoc network is secure or not. Further when we want to examine the security state of the mobile ad hoc network what should be enclosed in the security criteria for the mobile ad hoc network. So to evaluate the mobile ad hoc network is secure we commence in a few words the widely-used criteria.

1. Authenticity

To guarantee that participants in communication are genuine and not impersonators Authenticity has actual effect. To guarantee authencity it is necessary for the communication participants to verify their identities as what they have claimed using some techniques. The opponent could masquerade as a gentle node and thus get right to use to confidential resources, or even disseminate some fake messages to disturb the normal network operations if there is not such an authentication mechanism.

2. Confidentiality

Confidentiality is that certain information or data is only accessible to those who is authorized to access it. To maintain some confidentiality we need to keep information secret from all entities that do not have the privilege to access them.

3. Integrity

Integrity guarantees the identity of the messages when they

are transmitted between sender and receiver. Integrity can be compromised mainly in two ways:

a) Malicious altering:- A message can be replayed, modified or removed by an intruder with malicious goal, which is regarded as malicious altering.

b) Accidental altering:- if the message or data is vanished or its content is altered due to some gentle failures, which may be transmission errors in communication, hardware errors such as hard disk failure, then it is called as accidental altering.

4. No repudiation

No repudiation ensures that the sender and the receiver of a message cannot deny that they have sent or received such a message. If a node recognizes that the message it has received is erroneous, it can then use the incorrect message as a proof to alert other nodes that the node sending the inappropriate message should have been compromised [8].

5 Availability

The phrase *Availability* means that a node should sustain its ability to make available all the designed services and resources apart from the security status of it. Denial-of-service attacks mainly challenge the security criteria, where every nodes in the network can be the attack intention and thus some selfish and malicious nodes make some of the network resources and services occupied, for e.g.:- the key management service.

6. Authorization

Authorization is a method in which an individual is issued a official document, which specifies the permissions and privileges it has and cannot be fallacious, by the certificated authority. It is used to allocate special and various access rights to different level of users. For example, we need to make certain that function of network management should only accessible by the network administrator. Thus before the network administrator accesses the network management functions there should be an authorization process [9].

7. Anonymity

Anonymity means that each and every information that can be used to recognize the current user of the node should not be circulated by the node itself or the system software and hence kept private. This condition is intimately associated to privacy preserving, where we try to protect the nodes privacy from arbitrary exposé to any other entities.

8. Security Criteria: Summary

To guarantee the security of the mobile ad hoc network here we have discussed various core requirements that need to be achieved. Besides, there are a number of other security criteria that are application-oriented and much more specialized, they are Byzantine Robustness, location privacy, and self-stabilization, all of these are interrelated to the mobile ad hoc network routing protocol [11].

6 Conclusion

In this research paper, we try to look over the security related issues in the mobile ad hoc networks, which may be a main interruption to the operation of it. The mobile ad hoc networks are much more prone to various and all kind of security risks, like Denial of service attack, intrusion, and information disclosure, these results due to the mobility and open media nature. As a result, the requirements of security needs in the mobile ad hoc networks are much higher than in the traditional wired networks. Here we initiate the various security solutions for the mobile ad hoc networks that should be kept in mind. Due to this security criteria and security techniques that can help to make the mobile ad hoc networks safer from internal security threats and external security threats.

Acknowledgment

We authors wish thank to our Principal Prof. M.L. Gupta for their support.

References

[1] Jun-Zhao Sun "Mobile Ad Hoc Networking: An Essential Technology for Pervasive Computing"
[2] Hang Zhao "Security for Ad Hoc Networks".
[3] M. Frodigh, P. Johansson, and P. Larsson. "Wireless ad hoc networking: the art of networking without a network," *Ericsson Review*, No.4, 2000, pp. 248-263.
[4] Data Integrity, from *Wikipedia, the free encyclopedia*, http://en.wikipedia.org/wiki/Data_integrity.
[5] Wenjia Li and Anupam Joshi "Security Issues in Mobile Ad Hoc Networks - A Survey"
[6] Anuj Joshi1, Paa llavi Srivastava and Poonam Singh" Security Threats in Mobile Ad Hoc Network" S-JPSET: ISSN: 2229-7111, Vol. 1, Issue 2.
[7] Pravin Ghosekar, Girish Katkar Dr. Pradip Ghorpade "Mobile Ad Hoc Networking: Imperatives and Challenges" IJCA Special Issue on "Mobile Ad-hoc Networks" MANETs, 2010.
[8] M. Weiser, the Computer for the Twenty-First Century, *Scientific American*, September 1991.
[9] Hang Zhao "Security for Ad Hoc Networks".
[10] H. Deng, W. Li, Agrawal, D.P., "Routing security in wireless ad hoc networks," Cincinnati Univ., OH, USA; IEEE Communications Magazine, Oct. 2002, Volume: 40, page(s): 70- 75, ISSN: 0163-6804.
[11] J. Ahola, Ambient Intelligence, ERCIM (European Research Consortium for Information and Mathematics) NEWS, N. 47, October 2001.

Authors Information

1. **KRISHAN KANT LAVANIA**
Head, Department Of Information Technology
Arya Institute of Engineering & Technology, Kukas,

Jaipur, India.
k@lavania.in

2. **G.L. SAINI**
Student, M.Tech
glsaini86@gmail.com

3. **KOTHARI ROOSHABH H.**
Student, M.Tech
rooshabhkothari31@gmail.com

4. **YAGNIK HARSHRAJ A.**
Student, M.Tech
yagnik.harshraj@yahoo.co.in