SECURITY GOALS OF MANETs ALONG WITH RESEARCH CHALLENGES & ISSUES

Rajni Jain[1], Sohan Garg[2]

1. Research Scholar, Venkteshwara University-Gajraula Amroha (U.P.)
2. Professor, IIMT Management College-Meerut

Abstract: A mobile ad-hoc network (MANET) is a self-configuring infrastructure less network of mobile devices connected by wireless. *Ad hoc* is Latin and it means "for this purpose". Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet.

MANETs have the features like much lower mobility and much more stringent energy requirements. We analyze security goals of MANETs and will describe the research challenges and evaluate open issues in development of routing techniques in MANETs.

Keywords: QoS, MANETs, EMI

1. INTRODUCTION:

Wireless network refers to any type of computer network that is not connected by cables of any kind. It is a method by which homes, telecommunications networks and enterprise (business) installations avoid the costly process of introducing cables into a building, or as a connection between various equipment locations.[1] Wireless telecommunications networks are generally implemented and administered using radio communication. This implementation takes place at the physical level (layer) of the OSI model network structure.

Mobile ad hoc networks (MANETs) consist of a collection of wireless mobile nodes which dynamically exchange data among themselves without the reliance on a fixed base station or a wired backbone network. MANET nodes are typically distinguished by their limited power, processing, and memory resources as well as high degree of mobility. In such networks, the wireless mobile nodes may dynamically enter the network as well as leave the network. Due to the limited transmission range of wireless network nodes, multiple hops are usually needed for a node to exchange information with any other node in the network. Thus routing is a crucial issue to the design of a MANET. In this paper, we specifically examine the issues of multipath routing in MANETs. Multipath routing allows the establishment of multiple paths between a single source and single destination node. It is typically proposed in order to increase the reliability of data transmission (i.e., fault tolerance) or to provide load balancing. Load balancing is of especial importance in MANETs because of the limited bandwidth between the nodes. We also discuss the application of multipath routing to support application constraints such as reliability, load-balancing, energy-conservation, and Quality-of-Service (QoS).

With recent performance advancements in computer and wireless communications technologies, advanced mobile wireless computing is expected to see increasingly widespread use and application, much of which will involve the use of the Internet Protocol (IP) suite. The vision of mobile ad hoc networking is to support robust and efficient operation in mobile wireless networks by incorporating routing functionality into mobile nodes. Such networks are envisioned to have dynamic, sometimes rapidly-changing, random, multi hop topologies which are likely composed of relatively bandwidth-constrained wireless links. Within the Internet community, routing support for mobile hosts is presently being formulated as "mobile IP" technology. This is a technology to support nomadic host "roaming", where a roaming host may be connected through various means to the Internet other than its well known fixed-address domain space. The host may be directly physically connected to the fixed network on a foreign subnet, or be connected via a wireless link, dial-up line, etc. Supporting this form of host mobility requires address management, protocol interoperability enhancements and the like, but core network functions such as hop-by-

hop routing still presently rely upon preexisting routing protocols operating within the fixed network. In contrast, the goal of mobile ad hoc networking is to extend mobility into the realm of autonomous, mobile, wireless domains, where a set of nodes--which may be combined routers and hosts--themselves form the network routing infrastructure in an ad hoc fashion.

In MANETs 3 communication between nodes is done through the wireless medium. Because nodes are mobile and may join or leave the network, MANETs have a dynamic topology. Nodes that are in transmission range of each other are called neighbors. Neighbors can send directly to each other. However, when a node needs to send data to another non-neighboring node, the data is routed through

a sequence of multiple hops, with intermediate nodes acting as routers. An example ad hoc network is depicted in Figure 1.

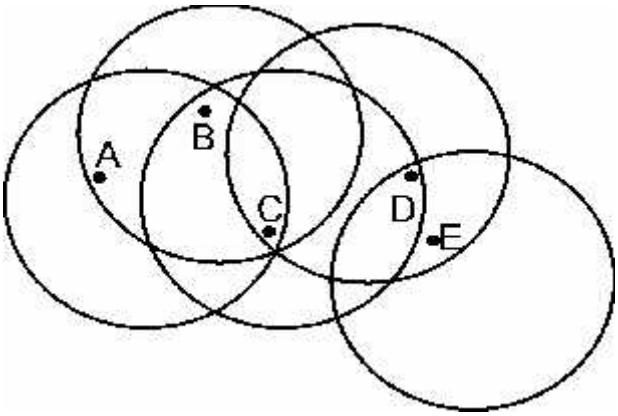

Fig. 1. An example ad hoc network, with circles representing nodes.

2. SECURITY GOALS OF MANETs:

Security involves a set of investments that are adequately funded. In MANET, all networking functions such as routing and packet forwarding, are performed by nodes themselves in a self-organizing manner. For these reasons, securing a mobile ad -hoc network is very challenging. The goals to evaluate if mobile ad-hoc network is secure or not are as follows:

2.1. Availability: Availability means the assets are accessible to authorized parties at appropriate times. Availability applies both to data and to services. It ensures the survivability of network service despite denial of service attack.

2.2. Confidentiality: Confidentiality ensures that computer-related assets are accessed only by authorized parties. That is, only those who should have access to something will actually get that access. To maintain confidentiality of some confidential information, we need to keep them secret from all entities that do not have privilege to access them. Confidentiality is sometimes called secrecy or privacy.

2.3. Integrity: Integrity means that assets can be modified only by authorized parties or only in authorized way. Modification includes writing, changing status, deleting and creating. Integrity assures that a message being transferred is never corrupted.

2.4. Authentication: Authentication enables a node to ensure the identity of peer node it is communicating with. Authentication is essentially assurance that participants in communication are authenticated and not impersonators. Authenticity is ensured because only the legitimate sender can produce a message that will decrypt properly with the shared key.

2.5. Non repudiation: Non repudiation ensures that sender and receiver of a message cannot disavow that they have ever sent or received such a message This is helpful when we need to discriminate if a node with some undesired function is compromised or not.

2.6. Anonymity: Anonymity means all information that can be used to identify owner or current user of node should default be kept private and not be distributed by node itself or the system software.

2.7. Authorization: This property assigns different access rights to different types of users. For example a network management can be performed by network administrator only.

3. RESEARCH ISSUES IN MANETs:

There are numerous issues to consider when deploying MANETs. The following are some of the main issues.

3.1. Unpredictability of environment: Ad hoc networks may be deployed in unknown terrains, hazardous conditions, and even hostile environments where tampering or the actual destruction of a node may be imminent. Depending on the environment, node failures may occur frequently.

3.2. Unreliability of wireless medium: Communication through the wireless medium is unreliable and subject to errors. Also, due to varying environmental conditions such as high levels of electro-magnetic interference (EMI) or inclement weather, the quality of the wireless link may be unpredictable.

Furthermore, in some applications, nodes may be resource-constrained and thus would not be able to support transport protocols necessary to ensure reliable communication on a lossy link. Thus, link quality may fluctuate in a MANET.

3.3. Resource-constrained nodes: Nodes in a MANET are typically battery powered as well as limited in storage and processing capabilities. Moreover, they may be situated in areas where it is not possible to re-charge and thus have limited lifetimes. Because of these limitations, they must have algorithms

which are energy-efficient as well as operating with limited processing and memory resources. The available bandwidth of the wireless medium may also be limited because nodes may not be able to sacrifice the energy consumed by operating at full link speed.

3.4. Dynamic topology: The topology in an ad hoc network may change constantly due to the mobility of nodes. As nodes move in and out of range of each other, some links break while new links between nodes are created. As a result of these issues,

MANETs are prone to numerous types of faults including,

(a) Transmission errors: The unreliability of the wireless medium and the unpredictability of the environment may lead to transmitted packets being garbled and thus received in error.

(b) Node failures: Nodes may fail at any time due to different types of hazardous conditions in the environment. They may also drop out of the network either voluntarily or when their energy supply is depleted.

(c) Link failures: Node failures as well as changing environmental conditions (e.g., increased levels of EMI) may cause links between nodes to break.

(d) Route breakages: When the network topology changes due to node/link failures and/or node/link additions to the network, routes become out-of date and thus incorrect. Depending upon the network transport protocol, packets forwarded through stale routes may either eventually be dropped or

be delayed; packets may take a circuitous route before eventually arriving at the destination node.

(e) Congested nodes or links: Due to the topology of the network and the nature of the routing protocol, certain nodes or links may become over utilized, i.e., congested. This will lead to either larger delays or packet loss. Routing protocols for MANETs must deal with these issues to be effective. In

the remainder of this section, we present an overview of some of the key uni path routing protocols for MANETs.

4. MANETs VULNERABILITY:

Vulnerability is a weakness in security system. A particular system may be vulnerable to unauthorized data manipulation because the system does not verify a user's identity before allowing data access. MANET is more vulnerable than wired network. Some of the vulnerabilities are as follows:-

4.1. Lack of centralized management: MANET doesn't have a centralized monitor server. The absence of management makes the detection of attacks difficult because it is not east to monitor the traffic in a highly dynamic and large scale ad-hoc network. Lack of centralized management will impede trust management for nodes.

4.2. Resource availability: Resource availability is a major issue in MANET. Providing secure communication in such changing environment as well as protection against specific threats and attacks, leads to development of various security schemes and architectures. Collaborative ad-hoc environments also allow implementation of self-organized security mechanism.

4.3. Scalability: Due to mobility of nodes, scale of ad-hoc network changing all the time. So scalability is a major issue concerning security. Security mechanism should be capable of handling a large network as well as small ones.

4.4. Cooperativeness: Routing algorithm for MANETs usually assumes that nodes are cooperative and non-malicious. As a result a malicious attacker can easily become an important routing agent and disrupt network operation by disobeying the protocol specifications.

4.5. Dynamic topology: Dynamic topology and changeable nodes membership may disturb the trust relationship among nodes. The trust may also be disturbed if some nodes are detected as compromised. This dynamic behavior could be better protected with distributed and adaptive security mechanisms.

4.6. Limited power supply: The nodes in mobile ad-hoc network need to consider restricted power supply, which will cause several problems. A node in mobile ad-hoc network may behave in a selfish manner when it is finding that there is only limited power supply.

4.7. Bandwidth constraint: Variable low capacity links exists as compared to wireless network which are more susceptible to external noise, interference and signal attenuation effects.

4.8. Adversary inside the Network: The mobile nodes within the MANET can freely join and leave the network. The nodes within network may also behave maliciously. This is hard to detect that the behavior of the node is malicious. Thus this attack is more dangerous than the external attack. These nodes are called compromised nodes.

4.9. No predefined Boundary: In mobile ad- hoc networks we cannot precisely define a physical boundary of the network. The nodes work in a nomadic environment where they are allowed to join and leave the wireless network. As soon as an adversary comes in the radio range of a node it will be able to communicate with that node. The attacks include

Eavesdropping impersonation; tempering, replay and Denial of Service (DoS) attack [2].

5. RESEARCH CHALLENGES OF MANETs:

The major challenges faced by the MANETS can be broadly classified as:

5.1. In incorporating emerging wireless network elements such as MDs, ad-hoc routers and embedded sensors in the existing protocol framework and

5.2. To provide end-to-end service abstractions that facilitates application development. These challenges are posed by a broad range of environments such as cellular data services, WiFi hot-spots, Info stations, mobile peer-to-peer, Ad-hoc mesh networks for broadband access, vehicular networks, sensor networks and pervasive systems. These wireless application scenarios lead to a diverse set of service requirements for the future Internet as summarized below:

(a) Naming and addressing flexibility.

(b) Mobility support for dynamic migration of end-users and network devices.

(c) Location services that provide information on geographic position.

(d) Self-organization and discovery for distributed control of network topology.

(e) Security and privacy considerations for mobile nodes and open wireless channels.

(f) Decentralized management for remote monitoring and control.

(g) Cross-layer support for optimization of protocol performance.

(h) Sensor network features such as aggregation, content routing and in-network Processing.

(i) Cognitive radio support for networks with physical layer adaptation.

(j) Economic incentives to encourage efficient sharing of resources. Taken together, the above MANET requirements represent a spectrum of network

challenges. During the last few years, almost every aspect of MANET has been explored to some level of detail. Yet, more questions have arisen than been answered. The major open problems are listed as:

(A) Autonomous: No centralized administration entity is available to manage the operation of the different mobile nodes.

(B) Dynamic topology: Nodes are mobile and can be connected dynamically in an arbitrary manner. Links of the network vary timely and are based on the proximity of one node to another node.

(C) Device discovery : Identifying relevant newly moved in nodes and informing about their existence need dynamic update to facilitate automatic optimal route selection.

(D) Bandwidth optimization: Wireless links have significantly lower capacity than the wired links.

(E) Limited resources: Mobile nodes rely on battery power, which is a scarce resource. Also storage capacity and power are severely limited.

(F) Scalability: Scalability can be broadly defined as whether the network is able to provide an acceptable level of service even in the presence of a large number of nodes.

(G) Limited physical security: Mobility implies higher security risks such as peer-to-peer network architecture

or a shared wireless medium accessible to both legitimate network users and malicious attackers. Eavesdropping, spoofing and denial-of-service attacks should be considered.

(H) Infrastructure-less and self operated: Self healing feature demands MANET should realign itself to blanket any node moving out of its range.

(I) Poor Transmission Quality: This is an inherent problem of wireless communication caused by several error sources that result in degradation of the received signal.

(J) Ad hoc addressing: Challenges in standard addressing scheme to be implemented.

(K) Network configuration: The whole MANET infrastructure is dynamic and is the reason for dynamic connection and disconnection of the variable links.

(L) Topology maintenance: Updating information of dynamic links among nodes in MANETs is a major challenge.

6. CONCLUSION & FUTURE SCOPE:

MANETs, the most talked about term in wireless technologies, approach to be the emperor of future *airs* provided the vision of “anytime, anywhere” communications. At present, the general trend is toward mesh architecture and large scale. New applications call for both bandwidth and capacity, which implies the need for a higher frequency and better spatial spectral reuse. Propagation, spectral reuse, and energy issues support a shift away from a single long wireless link (as in cellular) to a mesh of short links (as in MANET). Research on “multi-hop” architecture showed it a promising

solution to the implementation of ad hoc networks. As the evolvement goes on, especially the need of dense deployment such as battlefield and sensor networks, the nodes in MANET will be smaller, cheaper and capable.

7. REFERENCES:

1. Basagni, S., Conti, M., Giordano S., and Stojmenovic, I. (Eds.) Ad Hoc Networking. IEEE Press Wiley, New York, 2003.

2. Chlamtac, I., Conti, M., and Liu, J. J.-N. Mobile ad hoc networking: imperatives and challenges. *Ad Hoc Networks*, **1**(1), 2003, pp. 13–64.

3. Freebersyser, J. A., and Leiner, B. A DoD perspective on mobile ad hoc networks. In: Perkins, C. (Ed.) Ad Hoc Networking, Addison Wesley, Reading, MA, 2001, pp. 29–51.

4. IETF MANET Working Group. http:// www.ietf.org/html.charters/manetcharter. html

5. Toh, C-K. Ad Hoc Mobile Wireless Networks: Protocols and Systems. Prentice Hall, 2002.

6. Corson, S., and Macker, J. Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations. RFC 2501, IETF, Jan. 1999.

7. Abolhasan, M., Wysocki, T., and Dutkiewicz, E. A review of routing protocols for mobile ad hoc networks. *Ad Hoc Networks*, **2**(1), 2004, pp. 1–22.

8. Royer, E., and Toh, C. A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks. *IEEE Personal Communications*, **6**(2), Apr. 1999, pp. 46–55.

9. Hoebeke, J., Moerman, I., Dhoedt, B., and Demeester, P. Towards adaptive ad hoc network routing. *International Journal of Wireless and Mobile Computing*: Special Issue on 'Wireless Ad Hoc Networking', to be published.

10. Kozat, U. C., and Tassiulas, L. Service discovery in mobile ad hoc networks: an overall perspective on architectural choices and network layer support issues. *Ad Hoc Networks*, **2**(1), 2004, pp. 23–44.

11. Nilsson, A., and Tuominen, A. J. Internet Connectivity for Mobile Ad Hoc Networks. *Wireless Communications and Mobile Computing*, **2**(5), Aug. 2002, pp. 465–482.

12. Gupte, S., and Singhal, M. Secure routing in mobile wireless ad hoc networks. *Ad Hoc Networks*, **1**(1), 2003, pp. 151–174.

13. Buttyan, L., and Hubaux, J. P. Stimulating cooperation in self-organizing mobile ad hoc networks. *Mobile Networks and Applications*: Special Issue on Mobile Ad Hoc Networks, **8**(5), 2003.