ISSN 1512-1232

ANALYSIS OF SECURITY REQUIREMENTS IN WIRELESS NETWORKS AND MOBILE AD-HOC NETWORKS

Nipun Sharma
Lecturer (ECE Department), Chitkara University, Baddi, H.P, India

Abstract

The Wireless standard for LAN (802.11) gives the description of the access method, modulation, and authentication schemes and protocols to be followed. These standards face many challenges in the Mobile Ad-Hoc Network environment because of the constant node mobility and topology changes that it has to adapt to. This paper reviews the security concerns related to MANETs and their comparative analysis with the standard wireless networks.

1. Introduction

A mobile ad-hoc network (MANET) is a self-configuring network of mobile routers and associated hosts connected by wireless links. In MANETs, nodes do not have a priori knowledge of topology of network around them, they have to discover it. MANETs use limited network management and administration, in order to establish communications, dynamically. These algorithms need to keep routing table reasonably small, choose best route for given destination (fastest, most reliable, highest throughput, or cheapest route) and keep table up-to-date when nodes move or join. It uses network resilience parameters like latency, power consumption, & node status, route determination as a design criterion in order to ensure the integrity of network services in the event of component failures, traffic congestion and various other adverse conditions.

In MANET'S the routers are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger Internet. Minimal configuration and quick deployment make ad hoc networks suitable for emergency situations like natural or human-induced disasters, military conflicts, emergency medical situations etc.

1.1 Ad-hoc Network

A mobile ad hoc network is a collection of digital data terminals equipped with wireless transceivers that can communicate with one another without using any fixed networking infrastructure. Communication is maintained by the transmission of data packets over a common wireless channel. The absence of any fixed infrastructure, such as an array of base stations, makes ad hoc networks radically different from other wireless LANs. Whereas communication from a mobile terminal in an "infrastructure" network, such as a cellular network, is always maintained with a fixed base-station, a mobile terminal (node) in an ad hoc network can communicate directly with another node that is located within its radio transmission range. In order to transmit to a node that is located outside its radio range, data packets are relayed over a sequence of intermediate nodes using a store-and-forward "multihop" transmission principle. All nodes in an ad hoc network are required to relay packets on behalf of other nodes. Hence, a mobile ad hoc network is sometimes also called a multihop wireless network.

Since no base stations are required therefore it can be managed quickly without infrastructure. Hence, such networks are ideally suited for applications where such infrastructure is either unavailable or unreliable. In case of MANETs, a routing protocol is the mechanism by which user traffic is directed and transported through the network from a source node to a destination node. The objectives include maximizing network performance from an application point of view, while minimizing the cost imposed on the network in terms of capacity. Quality of Service (QoS) routing is an essential part of QoS architecture. It is a routing mechanism under which paths for flows are determined on the basis of some knowledge of the resources available in the network as well as on the QoS requirements of the flows or connections. The interest in this area grew rapidly in the nineties due to the popularity of a large number of portable digital devices such as laptop and palmtop computers, and the common availability of wireless communication devices. In this paper we discuss the security requirements in MANETs and design issues for routing protocols

2. Security Requirements

Security is a term that is liberally used in computer networks terminology. In this section we will go over the several attributes and terms that define security. The basic security needs of wireless ad hoc networks are more or less the same as those of wired networks. To some extent, several security schemes of the wire-line networks have been developed and implemented in wireless cellular networks. To make ad hoc networks secure, we need to find ways to incorporate some of these schemes of wireless and wire-line networks. In the following, we briefly introduce the standard terms, which are used when security aspects of a network are discussed.

(a) Availability

The services provided by a node continue to be provided irrespective of attacks. Nodes should be available for communication at all times. In other words, availability ensures survivability of the network services in presence of denial-of-service (DoS) attacks, which can be launched at any layer of an ad hoc network through radio jamming or battery exhaustion.

(b) Authenticity

This is essentially a confirmation that parties, in communication with each other, are genuine and not impersonators. This would require the nodes to some how prove that their identities are what they claim to be. Without authentication, an adversary could very well masquerade a node, could get access to sensitive and classified information, and could even interfere with the normal and secure network operation.

(c) Confidentiality

This ensures that information is not disclosed to unauthorized entities, i.e., an outsider should not be able to access information in transit between two nodes. Confidentiality necessitates the prevention of intermediate and non-trusted nodes from understanding the content of the packets being transmitted.

(d) Integrity

This is the guarantee that the message or packet being delivered has not been modified in transit or otherwise, and that what has been received is what was originally sent. A message could be corrupted owing to non-malicious reasons, such as radio propagation impairment, but there is always the possibility that an adversary has maliciously modified the content of the message.

(e) Non-repudiation

The sender of a message cannot later deny sending the information or the receiver cannot deny the reception. This can come in handy while detecting and isolating compromised nodes. Any node, which receives an erroneous message, can accuse the sender with proof and thus, convince other nodes about the compromised node. Routers cannot repudiate ownership of routing protocol messages they send.

(e) Ordering

Updates received from routers are in order, the non-occurrence of which can affect the correctness of routing protocols. Messages may not reflect the true state of the network and may propagate false information.

(f) Timeliness

Routing updates should be delivered in a timely fashion. Update messages that arrive late may not reflect the true state of links or routers on the network. They can cause incorrect forwarding or even propagate false information and weaken the credibility of the update information.

(g) Isolation

This requires that the protocol be able to identify misbehaving nodes and make them unable to interfere with routing. Alternatively, the routing protocol should be designed to be immune to malicious nodes.

(h) Authorization

An authenticated user or node is issued an unforgeable credential by the certificate authority. These credentials specify the privileges and permissions associated by the users or the nodes. Currently, credentials are not used in routing protocol packets, and any packet can trigger update propagations and modifications to the routing table.

(i) Lightweight computations

Many devices connected to an ad hoc network are assumed to be battery powered with limited computational abilities. Such a node cannot be expected to be able to carry out expensive computations. If operations such as public key cryptography or shortest path algorithms for large networks prove necessary, they should be confined to the least possible number of nodes; preferably only the route end points at route creation time.

(j) Location privacy

Often, the information carried in message headers is just as valuable as the message itself. The routing protocol should protect information about the location of nodes in a network and the network structure.

(k) Self-stabilization

A routing protocol should be able to recover automatically from any problem in a finite amount of time without human intervention. That is, it must not be possible to permanently disable a network by injecting a small number of malicious packets. If the routing protocol is self-stabilizing, an attacker who wishes to inflict continuous damage must remain in the network and continue sending malicious data to the nodes, which makes the attacker easier to locate.

(l) Byzantine robustness

A routing protocol should be able to function correctly even if some of the nodes participating in routing are intentionally disrupting its operation. Byzantine robustness can be seen as a stricter version of the self-stabilization property: the routing protocol must not only automatically recover from an attack; it should not cease from functioning even during the attack.

(m) Anonymity

Neither the mobile node nor its system software should expose any information that allows any conclusions about the owner or current user of the node. In case device or network identifiers are used (e.g. MAC address, IP address), no linking should be possible between the respective identifier and the owner’s identity for the communication partner or any outside attacker.

(n) Key management

The services in key management must provide solutions to the following questions:

*Trust model – how many different elements in the network can trust each other and trust relationships between network elements;

* Cryptosystems – while public-key cryptography offers more convenience, public-key cryptosystems are significantly slower than their secret-key counterparts when a similar level of security is needed;

* Key creation – which parties are allowed to generate keys to themselves or other parties, and what kind of keys;

* Key storage – any network element may have to store its own key and possibly keys of other elements as well, while in systems with shared keys with parts of keys distributed to several nodes, the compromising of a single node does not yet compromise the secret keys;

* Key distribution – generated keys have to be securely distributed to their owners, and any key that must be kept secret has to be distributed so that confidentiality, authenticity, and integrity are not violated.

(o) Access control

This consists of the means to govern the way the users or virtual users such as operating system processes (subjects) can have access to data (objects). Only authorized nodes may form, destroy, join, or leave groups.

(p) Trust

If physical security is low and trust relationships are dynamic, then the probability of a security failure may rise rapidly. It is not difficult to see what happens if the suspicion of a security failure increases. If there is a reason to believe that a part of the nodes belonging to a network have been compromised, users will probably become more reluctant to trust the network.

3. Design Issues

There are various issues issues in designing a routing protocol. These are explained below:

a. Mobility: One of the most important property of ad_hoc wireless network is the mobility associated with the nodes. The mobility of nodes results in frequent path breaks, packet collisions, transient loops, state routing information and difficulty in resource reservation. A good routing protocol should be able to efficiently solve the above issues.

b. Bandwidth constraint: since the channel is shared by all the nodes in broadcast region(any region in which all nodes can hear all other nodes),the bandwidth available per wireless link depends on the number of nodes and the traffic they handle. Thus only a fraction of total bandwidth is available for every node.

c. Error-prone and shared channel: the bit error rate in a wireless channel is very high compared to that in its wired counterparts. Routing protocols designed for ad-hoc wireless network should take this into account. Consideration of the state of the wireless link, signal to noise ratio and path loss for routing in ad-hoc wireless networks can improve the efficiency of the routing protocol. A good routing should have built in mechanism for distributing the load uniformly across the network so that formation of regions where channel congestion is high can be avoided.

d.Other resource constraints: the constraints on resources such that computing power, battery power and buffer storage also limit the capability of a routing protocol.

4. Characteristics of an ideal routing protocol

a. It must be fully distributed, as centralized routing involves high control overhead and hence is not scalable.
b. It must be adaptive to frequent topology changes caused by the mobility of nodes.
c. Route computation and maintenance must involve a minimum number of nodes.
d. It must be localized, as global state maintenance involves a huge state propagation control overhead.
e. It must be loop free and free from state routes.
f. The number of packet collisions must be kept to a minimum by limiting the no. of broadcasts made by each node.
g. It must converge to optimal routs once the network topology becomes stable.
h. It must optimally use bandwidth, computing power, memory and battery power.
i. Every node in the network should try to stir information regarding the stable local topology only
j. It should be able to provide a certain level of quality of service as demanded by the applications.

5. Conclusion

Having discussed basics of the security needs for ad hoc networks, it becomes imperative to employ a suitable routing protocol that suffices both security and QoS in MANETS. It should be pointed out that security and quality of service are two distinct attributes that are independent of each other in general. In summary, we can safely say that the mandatory security requirements include confidentiality, authentication, integrity, and non-repudiation. These would, in turn, require some form of cryptography, certificates, and signatures. Some other ideal characteristics include user authentication, explicit transaction authorization, end-to-end encryption, accepted log-on security (biometrics) instead of separate personal identification numbers (PINs) and passwords, intrusion detection, access control, logging, audit trail, security policy that states the rules for access, anti-virus scanners for the content, firewall, etc. This discussion demarcates the various branches within security, per se, such as intrusion detection and prevention, key agreement, trust management, data encryption, and access control.

6. References

1. Z. J. Haas, M. Gerla, D. B. Johnson, et al., ‘‘Guest editorial,’’ IEEE J. Select.Areas Commun., Special issue on wireless networks, vol. 17, no. 8, Aug. 1999,pp. 1329–1332.
2. D. B. Johnson and D. A. Maltz, ‘‘Protocols for adaptive wireless and mobile networking,’’ IEEE Personal Commun., Feb. 1996, pp. 34–42.
3. C. Bisdikian, ‘‘An overview of the Bluetooth wireless technology,’’ IEEE Commun. Mag., Dec. 2001, pp. 86–94. (For additional sources of comprehensive information on Bluetooth, see the official websites, www.bluetooth.com/ and www.bluetooth.org/; an excellent compendium of tutorials and references is available at http://kjhole.com/Standards/Intro.html.)
4. F. Bennett, D. Clarke, J. B. Evans, et al., ‘‘Piconet: embedded mobile networking,’’ IEEE Personal Commun., vol. 4, no. 5, Oct. 1997, pp. 8–15.
5. K. J. Negus, J. Waters, J. Tourrilhes, et al., ‘‘HomeRF and SWAP: wireless networking for the connected home,’’ ACMSIGMOBILEMobile Computing and Commun. Rev., vol. 2, no. 4, Oct. 1998, pp. 28–37.
6. F. A. Tobagi and L. Kleinrock, ‘‘Packet switching in radio channels - part 2: the hidden terminal problem in carrier sense multiple-access and the busy tone solution,’’ IEEE Trans. Commun., vol. COM-23, Dec. 1985, pp. 1417–1433.
7. C. R. Lin and M. Gerla, ‘‘MACA/PR: an asynchronous multimedia multihop wireless network,’’ Proc. 16th Annual Joint Conf. IEEE Comp. Commun. Soc. (INFOCOM 1997), vol. 1, 1997, pp. 118–125.
8. J. L. Sobrinho and A. S. Krishnakumar, ‘‘Quality-of-service in ad hoc carrier sense multiple access wireless networks,’’ IEEE J. Select. Areas Commun., vol. 17, No. 8, Aug. 1999, pp. 1353–1414.
9. S. Chen and K. Nahrstedt, ‘‘An overview of quality-of-service routing for the next generation high-speed networks: problems and solutions,’’ IEEE Network, Nov.–Dec. 1998, pp. 64–79.
10. S. Basagni, M. Conti, S. Giordano, and I. Stojmenovic (Editors),Mobile Ad Hoc Networking, John Wiley and Sons, 2004.
11. M. Ilyas (Editor), The Handbook of Wireless Ad Hoc Networks, CRC Press, 2003.
12. C. S. Ram Murthy and B. S. Manoj, Ad Hoc Wireless Networks – Architecture and Protocols, Prentice Hall, 2004.
13. I. Stojmenovic (Editor), Handbook of Wireless Networks & Mobile Computing, John Wiley and Sons, 2002.

Article received: 2010-07-12