MAT JOURNALS

Journal of Android and IOS Applications and Testing

Volume 1 Issue 3

An Introduction to Mobile Computing: A Growth for Security

[1]G Selva Priya, [2]R Aswini, [1]T Primya, [1]V Suresh, [1]P Anitha

[1]Dr. N.G.P. Institute of Technology, Coimbatore, India
[2]IFET College of Engineering, Villupuram, India
E-mail: selvapriya@drngpit.ac.in

Abstract

As too many people fancy the disparate services brought by mobile computing, it is conformist a worldwide verge in today's world. At an equivalent time, securing mobile computing has been paid continuous increasing attention. During this article, the safety problems in mobile computing setting square measure mentioned. This paper helps to research the safety risks confronted by mobile computing and gift the present security mechanisms.

Keywords: *Services, confronted, mobile computing, security*

INTRODUCTION

The term of mobile computing is commonly accustomed describe this kind of technology, combining wireless networking and computing. Numerous mobile computing paradigms are developed, and a few of them are already in daily use for business work likewise as for private applications. Wireless personal space networks (WPANs), covering smaller areas (from some of centimeters to few meters) with low power transmission, may be accustomed exchange data between devices inside the reach of an individual. A WPAN may be simply fashioned by commutation cables between computers and their peripherals, serving to individuals do their everyday chores or establish location aware services. One noteworthy technique of WPANs may be a Bluetooth based mostly network. However, WPANs are unnatural by short

communication vary and cannot scale very well for an extended distance.

MOBILE COMPUTING AT A GLANCE

The previous couple of years have seen a real revolution within the telecommunications world. Besides the three generations of wireless cellular systems, omnipresent computing has been attainable thanks to the advances in wireless communication technology and availableness of the many light-weight, compact, transportable computing devices, like laptops, PDAs, cellular phones and electronic organizers [1].

ARCHITECTURE FOR MOBILE COMPUTING

The corresponding two architectures square measure unremarkably mentioned as infrastructure-less and infrastructure-based network Figure 1. Ad hoc network could be an assortment of wireless mobile hosts forming a short lived network while not the help of any centralized administration or customary support services frequently obtainable on the wide space network [2]. As a result of its inherent infrastructure-less and self-organizing properties, a poster hoc network provides a particularly versatile methodology for establishing communications in things wherever geographical or terrestrial constraints demand wholly distributed network system, like military pursuit, unsafe atmosphere exploration, intelligence police investigation and instant conference [3]. Whereas we tend to square measure enjoying the varied services brought by mobile computing, we have got to appreciate that it comes with a price: security vulnerabilities [4].

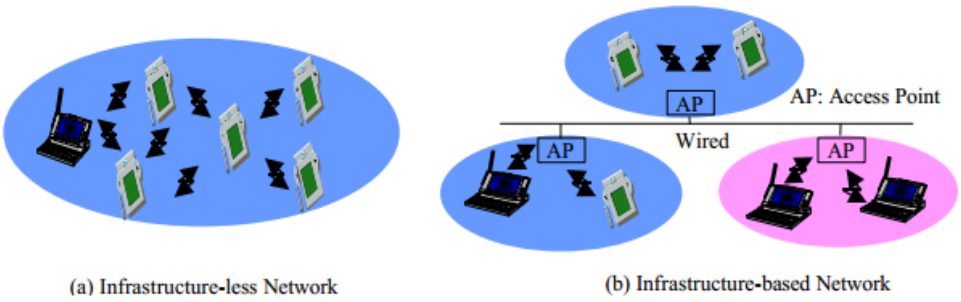

Fig. 1: *WLAN Architectures.*

SECURITY COUNTERMEASURES

Security Attributes

Secure mobile computing is critical in the development of any application of wireless networks. Security requirements similar to traditional networks, the goals of securing mobile computing can be defined by the following attributes: availability, confidentiality, integrity, authenticity and non-repudiation [5, 6].

- ***Availability*** ensures that the supposed network services are out there to the supposed parties once required.
- ***Confidentiality*** ensures that the transmitted info will solely be accessed by the supposed receivers and is rarely disclosed to unauthorized entities.
- ***Authenticity*** permits a user to make sure the identity of the entity it is human action with. While not authentication, associate individual will masquerade a legitimate user, therefore, gaining unauthorized access to resource and sensitive info and busy with the operation of users.
- ***Integrity*** guarantees that data is not corrupted throughout transmission.

Solely the approved parties are ready to modify it.

- ***Non-Repudiation*** ensures that associate degree entity will prove the transmission or reception of knowledge by another entity, i.e., a sender/receiver cannot incorrectly deny having received or sent sure knowledge.

Additional Security Requirements of Ad Hoc Networks

Ad hoc network may be a distributed network, within which network property and network services, as an example, routing, are maintained by the nodes themselves among the network. Every node has associate equal practicality. There are not any dedicated service nodes, which may work as a trustworthy authority to get and distribute the network keys or offer certificates to the nodes, because the certificate authority (CA) will within the ancient public key infrastructure (PKI) supported approaches. Although the service node will be outlined, keeping the supply of the service node to all or any the nodes in such a dynamic network is not a straightforward task. Moreover, with restricted physical protection, the service node is at risk of single purpose of failure, i.e., by solely damaging the service node, the total network would be paralytic [7–10]. Thus, distributed key generation and management approach is required to secure unintended networks.

CONCLUSION

Mobile computing technology provides anytime and anyplace service to mobile users by combining wireless networking and quality, which might engender numerous new applications and services. However, the inherent characteristics of wireless communication and also the demand for quality and movableness create mobile computing additional prone to numerous threats than ancient networks. Securing mobile computing is important to develop viable applications.

REFERENCES

1. LAN Standards of the IEEE Computer Society. Wireless LAN medium access control (MAC) and physical layer (PHY) specification.

IEEE Standard 802.11, 1999 Edition; 1999.

2. D. P. Agrawal, Q-A. Zeng. Introduction to wireless and mobile systems. Brooks/Cole Publisher; 2002.
3. J. Walker. Overview of IEEE 802.11b Security. http://www.intel.com/technology/itj/q22000/pdf/art_5.pdf.
4. N. Borisov, I. Goldberg, D. Wagner. Intercepting mobile communications: The insecurity of 802.11. http://www.isaac.cs.berkeley.edu/isaac/mobicom.pdf.
5. B. Dahill, B. N. Levine, E. Royer, et al. A secure routing protocol for ad hoc networks. Technical Report UM-CS-2001-037, Electrical Engineering and Computer Science, University of Michigan; 2001.
6. M. G. Zapata. Secure ad hoc on-demand distance vector routing. *ACM SIGMOBILE Mobile Computing and Communications Review*. 2002; 6(3): 106–107p.
7. Y. C. Hu, D. B. Johnson, A. Perrig. SEAD: Secure efficient distance vector routing in mobile wireless ad-hoc networks. *Proceedings of the 4th IEEE Workshop on Mobile Computing Systems and Applications (WMCSA '02)*. 2002; 3–13p.
8. Y. C. Hu, A. Perrig, D. B. Johnson. Ariadne: A secure on-demand routing protocol for ad hoc networks. *Proceedings of the 8th ACM International Conference on Mobile Computing and Networking, September*; 2002.
9. A. Perrig, R. Canetti, B. Whillock. TESLA: Multicast source authentication transform specification. http://www.ietf.org/internet-drafts/draft-ietf-msec-tesla-spec-00.txt; 2002.
10. L. Venkatraman, D. P. Agrawal. Startegies for enhancing routing security in protocols for mobile ad hoc networks. *JPDC Special Issue on Mobile Ad Hoc Networking and Computing*. 2003; 63(2): 214–227p.