M.E. Examination May 2009
Information Technology
5IT454: Secure Wireless Networks

Time:3hrs. **Max. Marks: 100**
Min. Pass Marks: 50

Note: Attempt all questions. All questions carry equal marks. Write answer of any two parts from each question.

Q.1 (a) What characteristics differentiate mobile computing from distributed computing? Give example to clearly distinguish among them. **10**

(b) What is the need of adaptation in mobile computing? How adaptation can be achieved through functionality and data. **10**

(c) (i) What is the importance of call to mobility ratio in the context of location management schemes? **10**
(ii) Explain security problems related to location management.

Q.2 (a) What is the difference between resource depletion versus resource exhaustion attack? Give example where (i) depletion is worse than exhaustion (ii) Exhaustion is worse than depletion. **10**

(b) (i) What makes a distributed denial of service attack more difficult to detect and defend against a normal denial of service attack? **10**
(ii) Describe three modes of security for Bluetooth devices.

(c) Describe four types of link keys used in Bluetooth? For what and how is each one used. **10**

Q.3 (a) Explain how WEP encryption, decryption and authentication work? **10**

(b) What are the flaws of WEP in the context of collision, weak key and reply attack? How did they get right? **10**

(c) What is the difference between 802.11, 802.11i and 802.11x protocols. **10**

Q.4 (a) What is the difference between the needs of local and metropolitan area network user? How is IEEE802.16 encryption similar to IEEE802.11i? **10**

(b) Why are sequential IV values better than random ones? Why would it not be easy to guess the next IV if they are used sequentially? **10**

(c) How is 802.16 extensible? What is the grace time and what happens if it is exceeded? **10**

Q.5 (a) Explain how authentication and encryption mechanism defined in GSM systems? **10**

(b) What are the problems with GSM security? **10**

(c) 3G systems are vulnerable to what kind of attacks? What are the weak points in 3G security? **10**