Sometimes the physically distributed computing devices in a network may be interested in computing some function of their private inputs without disclosing these inputs to one another. This type of computation falls under the category of Secure Multiparty Computation (SMC).

The solution to SMC problems in Mobile Ad hoc Networks (MANET) can be found with the modification of the data inputs or with some anonymization technique. MANETs are the wireless networks of the mobile computing devices with no support of any fixed infrastructure. The mobile nodes use any of the radio technology like Bluetooth, IEEE 802.11 or Hiperlan for directly communicating with each other. The nodes behave as hosts as well as routers. The security challenges in the MANET arise due to its dynamic topology, vulnerable wireless link and nomadic environment. An identification mechanism is needed between the nodes using identification and the credentials.

This security architecture simultaneously leads to privacy problems. Some mechanism is needed which prevents a node to learn the identity or the credentials of other nodes. To provide location privacy in MANET is a nontrivial task. Current routing protocols do not focus much on the security and the privacy issues. These aspects are postponed till further development. An authentication protocol is needed between nodes using some cryptographic technique. In service-oriented MANET the denial of the service must be taken care of so that the availability of the service is maintained.

The security requirement of the ad hoc network depends on its application. For example, for a simple business meeting the requirement is mitigated and for the military battlefield it is severe. Thus no general security architecture can be developed for MANET. Specific security architecture is needed for specific application. Much security related work is still pending and will add to the standards as the physical deployment of the MANET will grow. In this talk, an emphasis is made on how SMC solutions can be used for privacy preservation during computation.
Author’s Biography

Dr. Durgesh Kumar Mishra has received M.Tech. degree in Computer Science from DAVV, Indore in 1994 and PhD degree in Computer Engineering in 2008. Presently he is working as Professor (Computer Science and Engineering) and Dean (R&D) in Acropolis Institute of Technology and Research, Indore, MP, India.

He has some 21 years of teaching experience and more than 6 years of research experience. He has completed his research work with Dr. M. Chandwani, Director, IET-DAVV Indore, MP, India in Secure Multi-Party Computation for preserving Privacy. He has published more than 75 papers in refereed International/National Journal and Conference including IEEE, ACM etc and listed in DBLP, Citeseer, etc.

He is a Senior Member of IEEE and having responsibility of Chairman of IEEE Computer Society, Bombay Chapter, India and Vice Chairman of IEEE MP Subsection, India. Dr. Mishra has delivered his tutorials in IEEE International conferences in India as well as other countries also. He is also the programme committee member of several International conferences and Journals. He visited and delivered his invited talk in Taiwan, Bangladesh, Singapore, Nepal, USA, UK and several places in India in Secure Multi-Party Computation of Information Security for preserving privacy. He is an author of one book also. He is also the reviewer of four International Journals of Information Security. He is a Chief Editor of Journal of Technology and Engineering Sciences. He has been a consultant to industries and Government organization like Sale tax and Labor Department of Government of Madhya Pradesh, India.