Threshold based Authorization model for Authentication of a node in Wireless Mesh Networks

Divya Bansal
Department of Computer Science & Engineering, PEC University of Technology, Chandigarh.
Email: divya@pec.edu.in

Sanjeev Sofat
Department of Computer Science & Engineering, PEC University of Technology, Chandigarh
Email: sanjeevsofat@pec.ac.in

---ABSTRACT---

As various wireless networks evolve into the next generation to provide better services, a key technology, wireless mesh networks (WMNs), has emerged recently. There are number of issues in the deployment of WMNs. Amongst others security is quite a serious issue. Authenticating the users and devices in the network is a key point of network security. IEEE 802.11s mesh networks do not have any well defined or specified security architecture which can cater to large number of diversified applications. As the major characteristic of WMNs is multihop therefore using the 802.11i as the security standard is inadequate to provide security in Wireless Mesh Networks primarily because 802.11i was designed with the central security mechanism. In this paper a new approach using threshold authorization model with Clustered Certificate Authority is proposed which caters to the best of both the centralized and distributed architecture.

***Keywords*—Wireless Mesh networks, threshold authorization, secret key sharing.**

Date of Submission: 12, February 2010 Date of Acceptance: 8, April 2010

I. INTRODUCTION

NUMEROUS opportunities are being offered by emerging wireless technologies to develop quick infrastructures in order to immediately deploy important and useful community services. One big challenge is to provide a possibility to build a network that can grow in terms of coverage to offer service access (i.e. internet access) for a large number of people with different needs. Wireless Mesh Networks (WMNs) offer a solution with a promising future to this challenge. WMNs are undergoing rapid progress and inspiring numerous deployments as they deliver wireless services for a large variety of applications in Metropolitan Area Networks (MANs) and Local Area Networks (LANs). WMNs consist of mesh routers and mesh clients, where mesh routers have minimal mobility and form the backbone of WMNs. This architecture comprises of a set of access points (APs) interconnected using any of the wireless technologies i.e. Wi-Fi or Wi max etc. The wireless hot spot (coverage area of a single AP) in case of Wi-Fi and Wi max networks is up to 100 m and 48 Kms respectively. [1]

WMNs are however not ready for widescale deployment due to security challenges that specifies to kind of this kind of networks. The architecture inherits several authentication related problems being partially infrastructure less and open medium. This paper reviews the existing authentication technique for single hop WMNs highlighting its unsuitability for multi-hop scenarios. A new authentication scheme is proposed and its security analysis is carried out.

II. EXISITNG AUTHENTICATION MODELS

A. *Centralized Authentication Model*

Now we briefly discuss the centralized authentication model in WMNs. The implementation of AAA-server for authentication, authorization and accounting of users and devices can be inside the WMN (implemented in the mesh point) or it can be outside of WMN but accessible through an IP network via mesh portal. There is a little difference between authenticating a mesh point as well as mesh access point and a simple station. The authentication [8] is always performed with the server, but with the direct communication between mesh points. The basic theme of security association in centralized authentication model in a WMN is taken from the security association establishment in IEEE 802.11i. 802.11s [9, 10] WMN comprises the features of both ESS and IBSS configurations of IEEE 802.11i. As we know that 802.11s is implemented over the 802.11i security architecture, we assume that Authenticator and Supplicant part are implemented in each MP.

Hence, during each link establishment process, the ’802.11i Authentication and Key Management’ step includes two independent IEEE 802.1X authentication processes carried on with the server, each step resulting with a Pair wise Master Key Security Association. In first step, the IEEE/802.1X authentication between initiator mesh point(as supplicant) and the AS through peer mesh point (as authenticator) and in second step , IEEE/802.1X authentication between peer mesh point (as supplicant) and the AS through initiator mesh point (as authenticator). In a regular Pair wise Master Key Security Association establishment, an IEEE 802.1X/ EAP authentication is used.

As we know that WMNs are distributed in nature. Because of this distributive property of WMN, it requires some additional necessities on authentication. Such networks need to be self-organized and need to support distributed Authentication. One more fact is that the node mobility and rapid links they establish with neighboring nodes require freedom from central entities. The main reasons to go for distributed authentication because first, the centralized authentication server (AS) means every time when two mesh points wants to establish a link between them, and mutually authenticate [11] each other, they need to exchange the authentication information with the central authentication server. To complete this procedure having the WMN architecture in mind require multi-hop authentication capability to give the authentication information to the server every time when the peer mesh points are multi-hops away from the central AS. To provide such functionalities under the WMN environment where the link establishment rate is very high would definitely cause traffic congestion problems in the network. Second, the issue of single point of failure, the presence of a centralized AS means that during any mesh points authentication, the MP needs to provide authorization credentials to AS. The AS is hence the only entity in the network that can authenticate a new MP. In that case, if the AS breaks away, the authentication of new MPs to the network is impossible. Moreover, if the AS is compromised, the whole authorization scheme fails. At last the issue of saving credential, the presence of a centralized AS means that the AS is the only entity in the network that is able to verify the validity of the credentials that means saving the credentials of all authorized mesh points the central AS which is a very unpractical procedure in the case of a large scale network.

B. *Distributed Authentication Model*

As the Distributed authentication model is concerned there is no centralized AS and it can easily relate with the case of IBSS under 802.11i. The functions of server should be supported by each mesh point in the WMN. Therefore each mesh point should be able to act as Supplicant, Authenticator or as an Authentication Server during the authentication process. The same RSNA security association specifications are applied in the Distributed model as they were in the central model except for the central AS. Here the mesh points plays the role of Authentication Server as mentioned earlier. In every link establishment process the ’802.11i Authentication and Key management’ steps results with a pair wise master key security association, followed by pair wise transient key security association and group wise transient key security association. Every mesh node should establish a link, thus a table is required to handle multiple security associations that should be implemented in each mesh point.

When IEEE 802.1X authentication is used each mesh point requests its local IEEE 802.1X entity to create a Supplicant port for the peer MP. The Supplicant port will initiate the authentication to the peer MP by sending an EAPOL-Start message. The mesh point also request its local IEEE 802.1X entity to create an Authenticator port for the peer MP on receipt of an EAPOL-Start message. Upon initial authentication between any two mesh points, data frames, other than IEEE 802.1X messages, are not allowed to flow between the pair of MPs until both MPs in each pair of MPs have successfully completed Authentication and Key Management and have provided the supplied encryption keys. On the other hand everything has its own drawbacks so the distributed authentication model. In this model the trust is based on the transitivity that means any member of the WMN can issue a certificate for a new member if he trusts him. The certificates are issued to each other based on their personal relationships. Each time when two members want to authenticate each other, they look for a series of certificates (transitive) between them. Considering the WMN architecture this kind of chain-of-trust relationship can lead into situation of network congestion where the chain contain multi hop link between two end members. Permit one member to decide about the issuing of another member’s certificate also lead to a high probability of security breaches.

Going back to the IEEE 802.11s authentication schemes there are two kinds of authentication schemes: the centralized and the distributed schemes.

The centralized scheme requires that each device seeking access to the WMN should prove possession of a valid certificate to a Central Authentication Server. The link establishment between any two mesh nodes is possible only after a successful authentication of both devices to the Central Server using valid certificates. [1]. On the other hand, the distributed scheme requires that each device seeking access to the WMN should prove possession of a valid certificate to each MP with which it wants to establish a link. The link establishment between any two mesh nodes is possible only after a successful authentication of both devices to each other by exchanging and verifying valid certificates.

Drawbacks of existing models are follows:

a. Fully central
    i. Traffic congestion.

ii. What if Authentication server is compromised?

iii. Saving credentials of all Mesh Points at Authentication Server side is unpractical in case of large scale networks like WMNs.

b. Fully distributed

Transitive trust or chain of trust.

III. THE PROPOSED THRESHOLD AUTHORIZATION MODEL

A threshold authorization model with Clustered CA would stand midway between the two considered extreme models: It enforces a security policy that requires a K members' collaborative decision for issuing, renewing and revocation of certificates. Hence, the decision making is neither fully centralized nor fully distributed (Chain-of-trust case). In fact, a threshold authorization scheme employment in a WMN would ensure the distribution of trust among the network members, without relying on transitive trust. This way, the authorization privileges are neither restricted to one certification authority, however, they are not fully distributed in a way to allow one member to grant a valid certificate to a new user. [2]

Mesh network of 'n' nodes is considered. Each node has its own public/private key pair. One extra key pair is generated. Our software generates transparencies of key/image. Each node receives the transparency meant for it. When a new computer wants to become part of the wireless mesh network, it sends requests to the members of that network. Each contacted node encrypts the transparency with its private key and sends its public key with it (or public key can be announced in a different manner). The new computer decrypts the transparencies and combines them to form the original key.

If this key is same as original key the new computer is authorized and is added to the existing wireless mesh network.

The technique allows a black and white secret image to be divided as n image shares so that:

i. any k image shares (k = n) are sufficient to reconstruct the secret image in the lossless manner and

ii. any (k - 1) or fewer image shares cannot get enough information to reveal the secret image.

It is an effective, reliable and secure method to prevent the secret image from being lost, stolen or corrupted. In comparison with other image secret sharing methods, this approach's advantages are its large compression rate on the size of the image shares, its strong protection of the secret image and its ability for the real-time processing.

A. *Secret Sharing Schemes*

We now present a reliable image secret sharing method which incorporates two k-out-of-n secret sharing schemes:

i. Shamir's secret sharing scheme and

ii. Matrix projection secret sharing scheme.

The technique allows a colored secret image to be divided as n image shares so that: i) any k image shares (k = n) are suf?cient to reconstruct the secret image in the lossless manner and ii) any (k - 1) or fewer image shares cannot get enough information to reveal the secret image. It is an effective, reliable and secure method to prevent the secret image from being lost, stolen or corrupted. In comparison with other image secret sharing methods, this approach's advantages are its large compression rate on the size of the image shares, its strong protection of the secret image and its ability for the realtime processing.

B. *Shamir's Secret Sharing Scheme*

Shamir developed the idea of a (k, n) threshold-based secret sharing technique (k = n). The technique allows a polynomial function of order (k -1) constructed as, [7]

$$f(x)= d_0 + d_1 x + d_2 x^2 + ... + d_{k-1} x^{k-1} (\text{mod } p),$$

where the value d_0 is the secret and p is a prime number. The secret shares are the pairs of values (x_i, y_i) where $y_i = f(x_i)$, $1 = i = n$ and $0 < x_1 < x_2 ... < x_n = p - 1$. The polynomial function f(x) is destroyed after each shareholder possesses a pair of values (x_i, y_i) so that no single shareholder knows the secret value d0. In fact, no groups of k - 1 or fewer secret shares can discover the secret d0. On the other hand, when k or more secret shares are available, then we may set at least k linear equations $y_i = f(x_i)$ for the unknown d_i's. The unique solution to these equations shows that the secret value d_0 can be easily obtained by using Lagrange interpolation.

Shamir's Secret Sharing Scheme (SSS) is regarded as a Perfect Sharing Scheme (PSS) scheme because knowing even (k - 1) linear equations doesn't expose any information about the secret.

C. *Matrix Projection Secret Sharing Scheme*

Bai developed a SSS using matrix projection. The idea is based upon the invariance property of matrix projection. This scheme can be used to share multiple secrets, and detail of the scheme can be found in [6]. Here, we brie?y describe the procedure in two phases:

- Construction of Secret Shares from secret matrix S
  1. Construct a random m × k matrix A of rank k where m> 2(k - 1) - 1,
  2. Choose n linearly independent k×1 random vectors xi,
  3. Calculate share vi $=(A \times x_i)(\text{mod } p)$ for $1 = i = n$.
  4. Compute $S = (A(A'A)^{-1}A')(\text{mod } p)$,
  5. Solve $R = (S - \$)(\text{mod } p)$,
  6. Destroy matrix A, x_is, \$, S, and
  7. Distribute n shares v_i to n participants and make matrix R publicly known.

- Secret Reconstruction
  1. Collect k shares from any k participants, say the shares are $v_1, v_2, \ldots, v_k$ and construct a matrix B = [v1 v2 ... vk].
  2. Calculate the projection matrix S = (B(B’ B)$^{-1}$B’)(mod p),
  3. Verify that tr(S)= k, and
  4. Compute the secret S =(S + R (mod p)

IV. Implementation of the Scheme in the Network

A. *Construction of Secret Keys for Sharing*

i. There is an authentication server which distributes the keys to all the nodes. It has a secret key S which is used for the construction of the keys. The secret key is a m X m matrix.

ii. Initially it assumes a m X k matrix A with a rank k. Here m should be greater than 2k-3.

iii. Now it chooses n independent k X 1 vectors xi. Next vi is calculate using the formulae vi==(xi * A)mod p where 1<=i<=n.

iv. This gives us n keys that can be distributed among n nodes. (Fig 1)

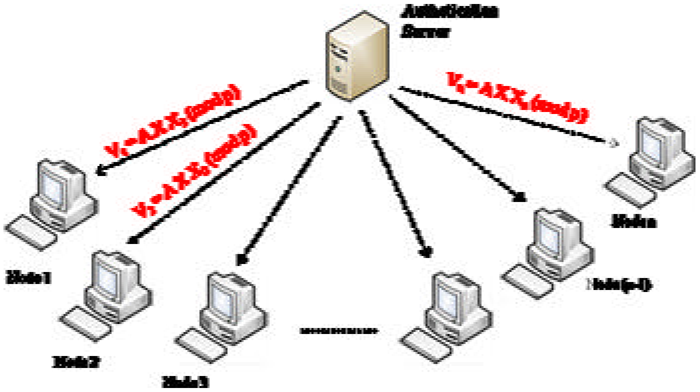

Figure 1: Construction of secret Keys

v. Now we need to calculate R that is made publically known which helps in authentication.

vi. For that initially the server computes T = (A(A’A)-1A’) (mod p).

vii. Next R is computed using the formulae
R = (S - T) (mod p).

viii. Now the server distributes all the keys and public key to all the nodes.

B. *Re-Construction of Secret Key for Authentication*

i. When a new node enters the network it contacts the nearest node. (Fig 2)

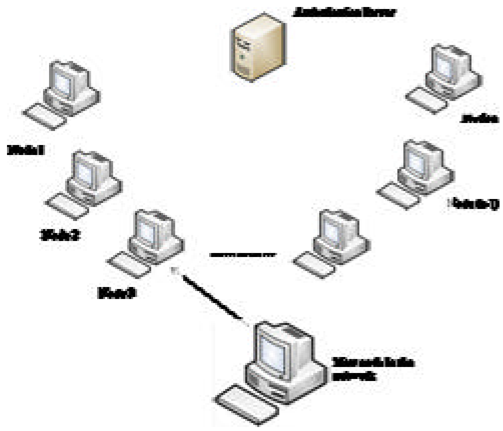

Figure 2: Entrance of new node

ii. This node communicates with all the other nodes. (Fig 3)

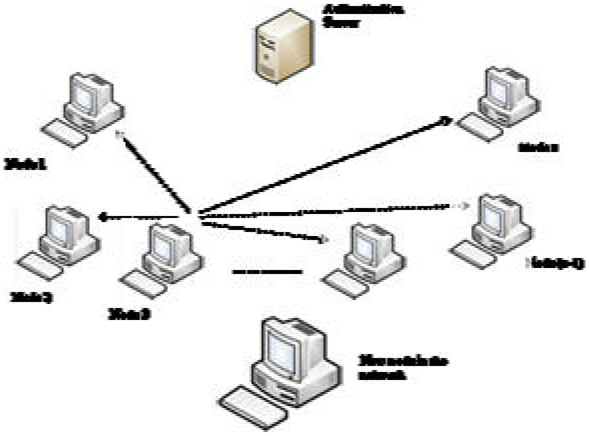

Figure 3: Inter-node Communication begins

iii. Then some of the nodes send their key to the authentication server to allow the new node. (Fig 4)

iv. If the number of nodes allowing is greater than or equal to threshold value k then the new node is allowed to enter otherwise not.

v. Let the server receives k keys. Le the keys be v1,v2…vk. Let B be a matrix such that
B = [v1 v2 . . . vk].

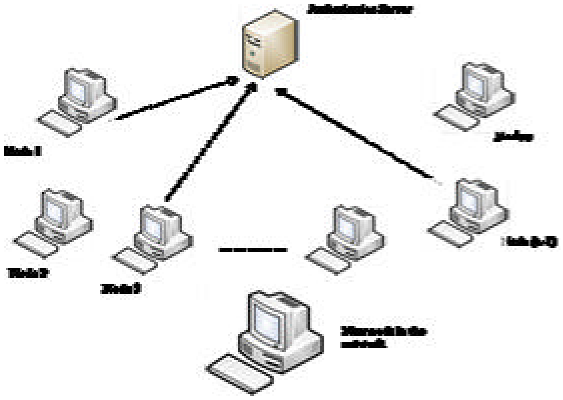

Figure 4: Node Communication with AS

vi. Using B the server calculates T=(B(B’B)-1B’) (mod p).

vii. Finally we calculate S using the formulae,

S = (T + R (mod p).

This gives the secret key S.

viii. Now the server matches this key with the original key. If both the key match the new node is allowed access in the network otherwise not.

ix. After the inclusion of the new node in the network, authentication generates the new shares as explained in the previous section. (Fig. 5)

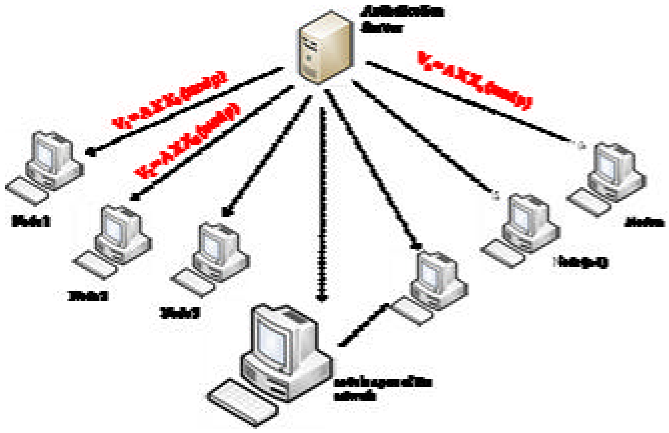
Authentication Server
$V_1=AXX_1(\text{mod } p)$
$V_2=AXX_2(\text{mod } p)$
$V_n=AXX_n(\text{mod } p)$
Node1
Node2
Node3
Node(n-1)
Noden

Figure 5: New node accepted in the network

V. Advantages over Existing Schemes

A. *Distributed Authorization*

Different roles played by the entities in the WMN can be configured as to support a range of applications that might include a centralized authorization, localized authorization (by means of Supervisors),or even a totally distributed authorization requiring K regular members.

B. *Threshold value for number of nodes required to authenticate*

The certification service we propose stands midway between the two considered extreme models: It enforces a security policy that requires a K members collaborative decision for issuing, renewing and revocation of certificates. Hence, the decision making is neither fully centralized nor fully distributed.

C. *Prevention of authentication of a node by a compromised node in WMN*

i. If a node in a WMN id hacked, or an attacker gets an access to become a part of the WMN, it may allow any number of new nodes to be a part of the same network. But, if the distributed policy is used, then, other (threshold number of nodes) nodes in the network are also required to authenticate the same. (Fig 6).

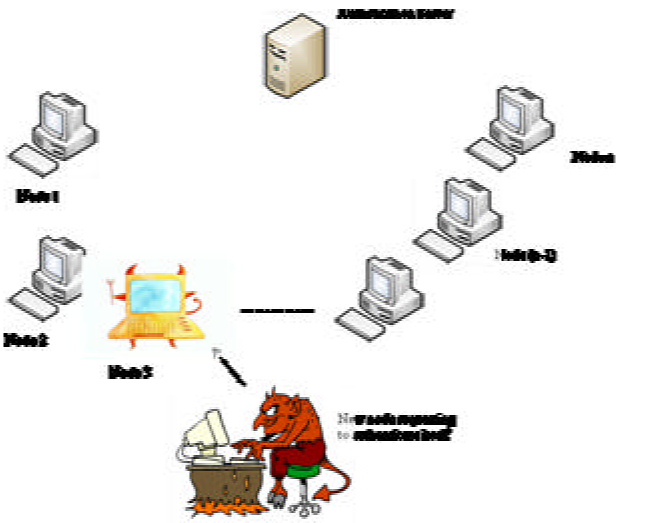

Figure 6: Compromised node attempts authentication

ii. Now, if the new node in the network (attacker), does not get the support of a minimum number of nodes (threshold value, k), the new node is denied the access into the network. (Fig 7)

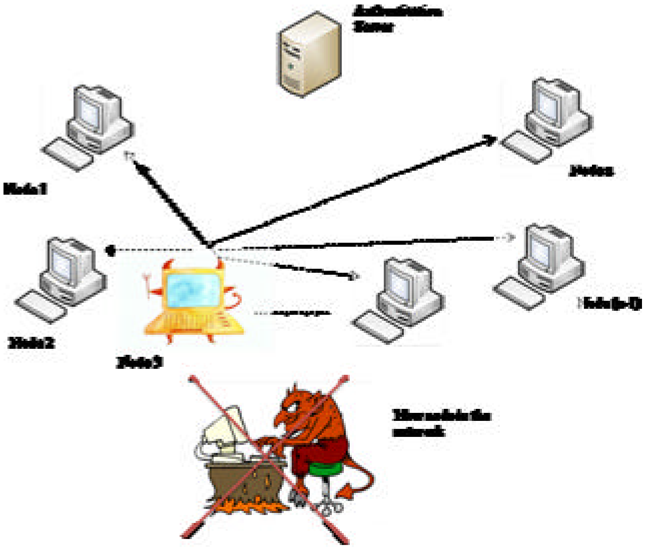

Figure 7: Compromised node denied access

VI. Conclusion

Security is the central issue of any network environment. Especially in the wireless communication the authentication is one of the most essential characteristic that should be considered very well. In the case of WMN the authentication becomes very critical issue to handle. However we have studied the Central and Distributed Authentication mechanism that can be applied in case of WMNs but there is more to do with it. Although the need for a distributed authorization service is necessary to cope with the WMN necessities, the challenge still resides in the establishment of trust inside the network. As explained before, a totally centralized approach is unlikely to be an ultimate solution for trust establishment inside a WMN. It is possible to establish a scheme in wireless meshed networks, where the entry of malicious bots can be restricted. The proposed scheme in this paper involves the use of threshold cryptography and uses the democratic principle that only if enough (threshold number) of nodes allow a new machine to enter, can it become a part of the wireless mesh network.

REFERENCES

[1] Kaleemullah Khan, and Muhammmad Akbar, “Authentication in Multi-Hop Wireless Mesh Networks”, Proceedings of World Academy of Science, Engineering and Technology, Volume 16, November 2006.

[2] Li Bai, Proceedings of the 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing, Pages: 31 - 36 , 2006, ISBN:0-7695-2539-3

[3] ECE Department, Temple University, Philadelphia, PA, U.S.A, “A Reliable (k, n) Image Secret Sharing Scheme”.

[4] Moni Naor and Adi Shamir, “Visual Cryptography”, Eurocrypt 94.

[5] Ivan Damgard, “Secret Sharing”, CPT 2006, ver 3, Lecture series

[6] Ronald Cramer, Ivan Damgard and Stefan Dziembowsk, “On the Complexity of Verifiable Secret Sharing and Multiparty Computation”, Proc. of STOC 2000

[7] L. Bai, “A strong ramp secret sharing scheme using matrix projection,” presented at the Second International Workshop on Trust, Security and Privacy for Ubiquitous Computing, Niagara-Falls, Buffalo, NY, 2006.

[8] A. Shamir, “How to share a secret,” Communications of the ACM, vol. 22, no. 11, pp. 612–613, Nov. 1979.

[9] Remote Authentication Dial In User Service (RADIUS). IETF RFC 2865, 2000

[10] The IEEE 802.11s Extended Service Set Mesh Networking Standard, Joseph D. Camp and Edward W. Knightly

[11] Principles of IEEE 802.11s, Guido R. Hiertz, Sebastian Max, Rui Zhao, Dee Denteneer, Lars Berlemann

[12] Yingfang Fu, Jingsha He, Rong Wang, Guorui Li,”Mutual Authentication in Wireless Mesh Networks”, Proc. of IEEE International Conference on Communications, ICC 2008, Beijing, China, 1690-1694

Authors Biography

Divya Bansal[F’79] is a Asst Professor and P.h.D student with PEC University of Technology, Chandigarh. She is the Associate Coordinator for Cyber security Research Centre, Chandigarh where she leads a research and development team working on MAC routing and secure protocols for wireless mesh networks. Her research interests also include cross-layer design and intrusion detection systems for wireless networks. She completed her M.E in Computer Science & Engineering from PEC University of Technology. Currently she is persuing her PhD. in the area of security in WMNs. Her current areas of research are Wireless Networks & Security.

Sanjeev Sofat [M’61] is a Distinguished Professor with PEC University of Technology, Chandigarh. He is the head of department of CSE and Information technology at PEC. He is also the Coordinator for Cyber Security Research Centre, Chandigarh. He also received his PhD. degree from Kurukshetra University in 2005.His current areas of research are Computer Networks & Information Security. He is a member of IEEE and CSI.