A FORMAL VERIFICATION FRAMEWORK FOR SECURITY POLICY MANAGEMENT IN MOBILE IP BASED WLAN

Soumya Maity[1] , P Bera[1] , S K Ghosh[1] , Pallab Dasgupta[2]

[1]School of Information Technology,
Indian Institute of Technology, Kharagpur, India
soumyam@iitkgp.ac.in, bera.padmalochan@gmail.com,
skg@iitkgp.ac.in
[2]Department of Computer Science and Engineering,
Indian Institute of Technology, Kharagpur, India
pallab@cse.iitkgp.ernet.in

ABSTRACT

The continuous advancement of wireless technologies especially for enterprise Wireless local area networks (LANs), demands well defined security mechanisms with appropriate architectural support to overcome various security loopholes. Implementing security policies on the basis of Role based Access Control (RBAC) models is an emerging field of research in WLAN security. However, verifying the correctness of the implemented policies over the distributed network devices with changes in topology, remains unexplored in the aforesaid domain. The enforcement of organizational security policies in WLANs require protection over the network resources from unauthorized access. Hence, it is required to ensure correct distribution of access control rules to the network access points conforming to the security policy. In WLAN security policy management, the standard IP based access control mechanisms are not sufficient to meet the organizational requirements due to its dynamic topology characteristics. In an enterprise network environments, the role-based access control (RBAC) mechanisms can be deployed to strengthen the security perimeter over the network resources. Further, there is a need to model the time and location dependent access constraints. In this paper, we propose a WLAN security management system supported by a formal spatio-temporal RBAC (STRBAC) model and a Boolean satisfiability (SAT) based verification framework. The concept of mobile IP has been used to ensure fixed layer 3 address mapping for the mobile hosts in a dynamic scenario. The system stems from logical partitioning of the WLAN topology into various security policy zones. It includes a Global Policy Server (GPS) that formalises the organisational access policies and determines the high level policy configurations for different policy zones; a Central Authentication & Role Server (CARS) which authenticates the users (or nodes) and the access points (AP) in various zones and also assigns appropriate roles to the users. Every host has to register their unique MAC address to a Central Authentication and Role Server(CARS). Each policy zone consists of an Wireless Policy Zone Controller (WPZCon) that coordinates with a dedicated Local Role Server (LRS) to extract the low level access configurations corresponding to the zone access router. We also propose a formal spatio-temporal RBAC (STRBAC) model to represent the global security policies formally and a SAT based verification framework to verify the access configurations

KEYWORDS

WLAN, Security Policy, Verification, Mobile IP

DOI : 10.5121/ijnsa.2010.2415

1. INTRODUCTION

The widespread deployment and dynamic topology characteristics of wireless networks make the security management in wireless networks (WLAN) increasingly difficult. Mobile users (with laptops and hand-held devices) remotely access the internal network from a public network zone; hence may violate the organisational security policies. Typically, organisational security policy provides a set of rules to access network objects by various users in the network. It requires a strong security policy management system with appropriate access control models to meet the organisational security need.

An enterprise LAN demands the security policies to be implemented over the distributed network for proper functionality of the policy based security management system. For policy based security management a primary concern is partitioning the network topology into different logical policy zones, and thus enforcing the security policies in the policy zones through a set of functional elements. It requires proper distribution of the system functionality (or functional rules) into various architectural elements. However, the deployment of policy based security management in wireless network (WLAN) require appropriate access control models (such as role-based access control (RBAC), spatio-temporal RBAC) for representing and enforcing the security policies. This is due to the dynamic topology characteristics of wireless networks as wireless nodes may not bind to a specific IP address. Due to the dynamic topology characteristics of wireless networks mobile IP is used. The mobile IP [17] is always specific to a host and does not change from location to location. The background and standards for policy based security management can be found in RFC 3198 [5]. The use of mobile IP to implement the security policy, which increases the performance of the system and gives better results compared to MAC based models as referred in [2] and [18].

Role based access control (RBAC) mechanisms are already being used for controlled access management in commercial organizations. In RBAC, permissions are attached to roles and users must be assigned to these roles to get the permissions for accessing the resources. Recently, temporal RBAC (TRBAC) and spatio-temporal RBAC (STRBAC) models are also evolved for location and time dependent access control. In wireless LAN security management, the STRBAC model can be used where the users associated to a role can access network objects, iff they satisfy certain location and time constraints. For example, in an academic network, Students are not allowed to access internet from their residential halls during class time (say, 08:00-18:00 in weekdays). However, they are always allowed to access internet from the academic departments.

- Home Agent is a designated router in the home network of the mobile node, maintains the mobility binding in a mobility binding table where each entry is identified by the tuple $< \alpha, \tau, \tilde{l} >$ where α is permanent home address, τ is temporary care-of address and $\tilde{l}$ is association lifetime.

- Foreign Agent are specialized routers on the foreign network where the mobile node is currently visiting. The foreign agent maintains a visitor list which contains information about the mobile nodes currently visiting that network. Each entry in the visitor list is identified by the tuple $< \alpha, \psi, w, \tilde{l} >$,where ψ is address of Home agent and w is MAC address of the mobile node. Foreign agent provides the new τ to a host.

- Central Authentication & Role Server (CARS) which authenticates the users (or nodes) and access points (AP) and also assigns appropriate roles to the users based on user credentials.

- Local Role Servers (LRS) corresponding to the respective policy zones are populated with the user-role information from the CARS.

- The Global Policy Server formally models the global security policy, GP; determines the high level policy configurations (represented as, < GPZ1 , ..., GPZN >) for various policy zones.
- The distributed Wireless Policy Zone Controllers (WPZCons) determine the low level access configurations (represented as, < LPZ1 , ..., LPZN >) coordinating with the local role servers and validates the access configurations with high level policy configurations.
- We propose a formal STRBAC model to represent the security policies and access configurations in the system.
- A SAT based framework has been presented to verify the low level access configuration with respect to the global policy.

The rest of the paper is organized as follows. The related work in the areas of Wireless LAN policy based security management and spatio-temporal RBAC models has been described in section 2. In section 3, we describe the architecture and operational flow of the proposed WLAN policy management system. Section 4 describes the proposed spatio-temporal RBAC model to support our policy management system. The analysis of the framework with a case study has been presented in section 5. Section 6 describes the SAT based verification procedure for analyzing the access configurations with respect to the global policy.

2. Related Work

Wireless networks are facing the premature stage of deployment of network policy based security management whereas several research has been performed in this area on wired LAN. Westrinen et al. [5] standardised the terminologies and functional elements for policy based management. The research outcome of IST-POSITIF project [1] is policy-based security framework in local area networks. The IETF Policy working group developed a framework for network policy based admission control [4]. It consists of a central policy server that interprets the policies, makes policy decisions and communicates them to various policy enforcement

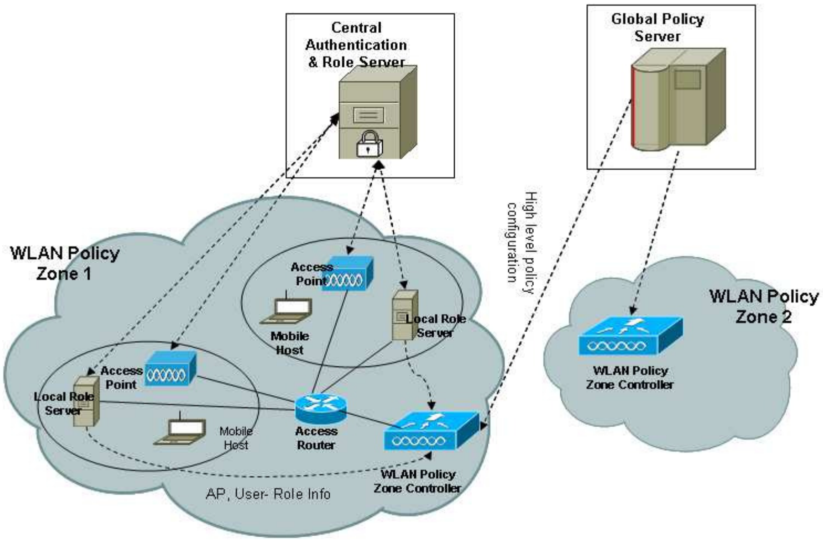

Figure 1: Wireless LAN Security Policy Management System

points. J Burns et al. propose a framework [3] for automatic management of network security policies based on central policy engine. The policy engine gets populated by the models of network elements and services, validates policies and computes new configurations for network elements when policies are violated. But, the framework considers very simple set of policy constraints. A recent work [2] has been proposed by Lapiotis et al. on policy based security management in wireless LAN. They propose a distributed policy based architecture which includes a central policy engine and distributed wireless domain managers with consistent local policy autonomy. But, they do not describe the type of security policies enforced and also do not describe the formal validation of the policies.

Role based access control (RBAC) model [6] is used for addressing the access requirements of commercial organizations. Several work has been done to improve RBAC functionalities incorporating time and location information. Joshi et al. [7] propose a Generalized Tempo- ral Role Based Access Control Model (GTRBAC) incorporating time to the RBAC model. Temporal constraints determine when the role can be enabled or disabled. In this work, the authors introduce the concept of time-based role hierarchy. GEO-RBAC [8] is an extension RBAC incorporating spatial information. Here, the roles are activated based on location. Ray and Toahchoodee [9] propose a Spatio-Temporal Role-Based Access Control Model incorporating both time and location information. We introduce the notion of wireless policy zone to represent location in our model. The role permissions to access network objects are modeled through policy rules containing both policy zone(location) and temporal constraints. RFC 4271 describes the working principles of mobile IP. The detail concept was elaborated in 1998 by Perkins [19]. Lapiotis et. al. [2] has proposed the policybsed management over link layer. This work was extended in our previous work [18]. The application of spatio-temporal RBAC model in wireless network security is in its infancy. Laborde et al. [11] presents a colored Petri Net based tool which allows to describe graphically given network topology, the security mechanism and the goals required. In this work, the authors model the security policies through generalized RBAC without considering time and location dependent service access. Moreover, the proposed tool is not applicable in wireless networks. To the best of our knowledge, the only work which uses spatio-temporal RBAC in wireless network is by Tomur and Erten [10]. They present a layered security architecture to control access in organizational wireless networks based STRBAC model using tested wired network components such as VPNs and Firewalls. However, this work does not describe the modeling of STRBAC policies using existing ACL standards. In our proposed WLAN policy management system, the global access policies are represented through a formal STRBAC model and implemented through distributed wireless policy zone controllers which outsource the high level policy configurations from the global policy server, derives correct low level access configuration and validates it. This makes the task of policy enforcement and validation easier and efficient.

3. WLAN Security Policy Management System

The proposed WLAN policy management system shown in Fig.1 stems from the notion of Wireless policy zones. A policy zone comprises of one or more wireless Access Points (AP), a dedicated Wireless Policy Zone Controller (WPZCon), a home agent(HA), a foreign agent(FA) and a Local Role Server (LRS) separated from other zones by a zone router.

The authentication of the users and the access points are managed by a special authentication server (AS) called Central Authentication & Role Server (CARS) which can be a RADIUS or an AAA server [16]. It also assigns appropriate roles to the authenticated users based on user credentials and policy zone (location) information. Each host is assigned with a IP address from a pool of IP addresses mapped with that Role. A home agent takes the responsibility to forward a packet to a host using the concept of Mobile IP [17]. Whenever new node comes in the range of an AP, AS authenticates it. LRS is informed about the new node getting associated the node in the corresponding zone. When a node leaves the range of an AP, using the baecon packet, AP can sense it and requests the AS to remove the information regarding the node from the zone. The LRS is responsible for maintaining the AP and user-role information in a policy zone. The Global Policy Server (GPS) formalises the global security policy (GP) through a spatio-temporal RBAC model. The detail of the STRBAC model is described in section 4. It also determines and validates high level policy configurations for various policy zones. Each WPZCon coordinate with the local role server to derive low level access configuration for the policy zone and validates it with corresponding high level configuration. Finally, the implementation access rules corresponding to the low level access configurations are distributed to various zone access points. The operational flow of the system is shown in Fig.2. In our framework, the distributed policy zone architecture makes the task of policy enforcement and validation easier and efficient. We also propose a formal spatio-temporal RBAC model for representing the security policies described in the next section.

4. Proposed Spatio-temporal RBAC Model for WLAN Policy Management

Typically, the spatio-temporal RBAC model incorporates the location and time information to the basic RBAC entities through various relations. The basic RBAC entities are users, roles, objects, permissions and operations. The modelling of location and time information to support the proposed WLAN policy management system has been described further below.

4.1 Modelling Location

In our model, the network location is represented in terms of policy zones. The policy zones physically represent different sections or units in an organisational WLAN. For example, in a typical Academic network, the policy zones can be Academic sections, Hostels or Administration. A policy zone is formally defined as follows:

Definition 1: [Policy Zone] A Policy Zone P is defined as a set of IP addresses or IP address block {I Pi , I Pj , ..., I Pn }. The IP addresses can be contiguous or discrete. Example of a contiguous IP address block is [10.14.0.0 – 10.14.255.255]. Example of a discrete IP address block is [10.14.0.0 – 10.14.255.255, 10.16.0.0 – 10.16.255.255]. A policy zone can contain another policy zone which is formalized as follows:

Definition 2: [Policy Zone Containment] A policy zone Zi is contained in another policy zone Zk , denoted as Zi ⊆ Zk , if the following condition holds: $\forall IP_j \in Z_i, IP_j \in Z_k$. The Zi and Zk are referred as contained and containing policy zones respectively.

4.2 Modelling Time:

The time must be modelled with appropriate granularity to provide temporal object access. The granularity of time may depend on the organisational access control requirements. To represent time in our model, we use the notion of time instant and time interval.

A time instant is a discrete point on the time line. A time interval is a set of time instances. The interval can be continuous and non-continuous. Example of a continuous interval is 09:00-15:00 on 24th July. Example of a non-continuous time interval is 09:00-19:00 on Monday to Friday in the month of July. A time instant ti in the interval T is indicated as ti ∈ T .

Two time intervals can be related by any of the following relations: disjoint, equality, and overlapping as mentioned in [10]. The time intervals Ti and Tj are disjoint if the intersection of the time instances in Ti with those of Tj results in a null set. Two time intervals Ti and Tj are equal if the set of time instances in Ti is equal to those of Tj . The time intervals Ti and Tj are overlapping if the intersection of the time instances in Ti with those of Tj results in a non-empty set. A special case of overlapping relation is referred to as containment. A time interval Ti is contained in another interval Tj if the set of time instances in Ti is a subset of those in Tj . The containment relation is denoted as Ti ^{1}Tj .

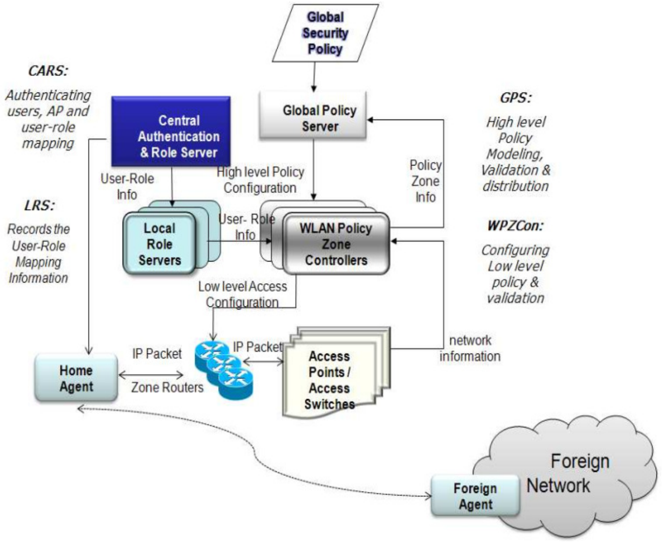
Global Security Policy
CARS:
Authenticating users, AP and user-role mapping
Central Authentication & Role Server
Global Policy Server
GPS:
High level Policy Modeling, Validation & distribution
User-Role Info
High level Policy Configuration
Policy Zone Info
LRS:
Records the User-Role Mapping Information
Local Role Servers
User- Role Info
WLAN Policy Zone Controllers
WPZCon:
Configuring Low level policy & validation
Low level Access Configuration
IP Packet
IP Packet
Access Points / Access Switches
network information
Home Agent
Zone Routers
Foreign Agent
Foreign Network

Figure 2: Operational Flow of the WLAN Security Policy Management System

4.3 Modelling Basic RBAC entities in the proposed System

The basic RBAC entities are Users, Roles, Objects, Permissions and Operations. In our model, Permissions and Operations associated to various roles are modelled as Policy Rules; whereas Users, Objects and Roles are modelled according to the context of the network.

Users: The users (or nodes) enters in a wireless policy zone tries to communicate to an wireless access point (AP) in the zone. The central authentication & role server (CARS) authenticates the users and the AP(s) based on user credentials (mainly, MAC address), locations (policy zones) and AP credentials (device ID and network-ID). The location of an user is the policy zone from which it communicates and that can change with time. The policy zone of an user u during time interval T can be identified by the function U serP Z one(u, T). Multiple users can be associated to a single policy zone at any given point of time.

Network Objects: In the proposed model, the network objects are logical. A network object is identified by a network service and a service policy zone.

Definition 3: [Network Object] A network object $Obj_i < Serv_j , Z_k >$ represents a net- work service $Serv_j$ associated to a service policy zone Z_k .

Network services refer to any network applications conforming to TCP/IP protocol. For example, some of the known network services are ssh, telnet, http etc. The service policy zone is the destination location associated to the service. For example, ssh service access to a policy zone Zd can be represented by a network object $Obj_i < ssh, Z_d >$.

Roles: Roles represent group of users. For example, typical roles for an academic institution may be faculty, student, administrator, guest etc. In our model, the assignment of roles to the users is location and time dependent. For example, an user can be assigned the role of faculty in academic policy zone at any time. Thus, valid users must satisfy the spatial and temporal constraints before role assignment. RoleAssignZ one(ri) represents the policy zone(s) where the role ri can be assigned. RoleAssignT ime(r_j) represents the time interval when the role r_j can be assigned. Some role r_k can be allocated anywhere. In that case RoleAssignZ

one(r_k) = Any. Similarly, we specify RoleAssignT ime(r_k) = Always, if some role rk can be assigned any time.
The predicate UserRoleAssign(u_i , r_j , T , Z_k) states that the user ui is assigned to role rj during the time interval T and policy zone Z_k . This predicate must satisfy the property: U serRoleAssign(u_i , r_j , T , Z_k) ⇒ (U serP Z one(u_i , T) = Z_k) ∧ (Z_k ⊆ RoleAssignZ one(r_j)) ∧ (T ⊆ RoleAssignT ime(r_j)).

4.4 Modelling Mobility

Each host, x has a home network where it belongs to. H (x), x ∈ theN/W address of home network is the Home agent of x which contains the tuple < α, τ, ˜1, ψ, w > (explained earlier) for each x. The foreign agent, F (x), X ∈ any network holds the information of the same tuple. After x, x ↔ α, being registered to F (x), Home agent gets the information about C O(x), C O(x) = f (F (x)) ∈ {address space of the network F(x) belongs to}. The function f defined on a foreign agent returns an IP address. In practise, F always polls its identity in link layer by broadcast message. x reads the data and send necessary data to be registered. F on the other hand registers C O(x) with the H (x). H (x) maps the address of x with C O(x) and forwards packets to C O(x) which are destined to x. So, each node after registering and getting authenticated gets an permanent IP (α) from a pool of addresses. It is assigned with the home agent from the zone it belongs to. When the node is in the home network, it gets all the packet bound to it normally through the gateway. When the nodes leaves to another zone, the Foreign agent(FA) gives it a temporary care of address (τ). FA sends the τ for the node to the corresponding HA. In this case all the packet destined to the node first comes to the home agent. HA then tunnels the packet to the temporary address of the node at that point of time. In brief,a mobile node can have two addresses, a permanent home address (α) and a care of address (τ) , which is associated with the network the mobile node is visiting. When any host wants to communicate with the mobile node, it uses the ψ (address of home agent) to send packets. These packets are intercepted by the home agent, which uses a table and tunnels the packets to the mobile node's care-of address with a new IP header, preserving the original IP header. The packets are decapsulated at the end of the tunnel to remove the added IP header and delivered to the mobile node.

When acting as sender, mobile node simply sends packets directly to the other communicating host through the foreign agent. This is known as triangular routing. In case of the networks whose gateway routers have ingress filtering enabled, the foreign agent would use reverse tunnelling by encapsulating mobile node's packets for the home agent, which in turn forwards them to the communicating node, because the source IP of the mobile host would need to belong to the subnet of the foreign network else the packets will be discarded by the router.

The Mobile IP protocol defines the following:

• an authenticated registration procedure by which a mobile node informs its home agent(s) of its care-of-address"(es)

• an extension to ICMP Router Discovery, which allows mobile nodes to discover prospec- tive home agents and foreign agents

• the rules for routing packets to and from mobile nodes, including the specification of one mandatory tunnelling mechanism and several optional tunnelling mechanisms.

4.5 Modelling of Global Policy

The global policy of an organisation can be modelled through a set of policy rules that “permit”/“deny” user accesses to various network objects from different policy zones during specified time intervals. A policy rule represents the network object accessibility permissions (“permit” or “deny”) of a role from a policy zone to the network objects during certain time interval.

Definition 4: [Policy Rule] A Policy Rule $PR_i < r_j , Z_l , Obj_k , T, p >$ defines that the role r_j is assigned the permission p (“permit”/“deny”) to access the object obj_k from the policy zone $PZon_l$ during the time interval T.

Each policy rule must satisfy the following predicates: (1) T c RoleAssignTime(r_j), i.e., time interval T must be contained in RoleAssignTime(r_j);
(2) Z_l c RoleAssignZone(r_j), i.e., source zone Z_l contained in RoleAssignZone(r_j). The global policy is represented as ordered set of policy rules $\{PR_1, ..., PR_N\}$.
Inter-rule Subsuming Conflicts and Resolution: The global policy model may contain inter-rule subsuming conflicts due to rule component dependencies. The rule components are source zone, object, role, time and permission. We define the inter-rule subsuming conflicts as follows.

Definition 5: [Inter-rule Subsuming Conflict] A pair of policy rules PR_X and PR_y are subsume-conflicting, iff (P R_X[obj] = P R_y [obj]) A (P R_X[role] = P R_y [role]) A (P R_X[P Z on] c PR_y [P Z on]) A (P R_X [T)] ¹ P R_y [T]), where c and ¹ indicate policy zone containment and time containment respectively.

Here, two cases may occur based on permission component of the rules.
Case 1: PR_X[permission(p)] = PR_y [permission(p)] and Case 2: PR_X[permission(p)] = PR_y [permission(p)]. Under each case, following subcases may appear. subcase(a): (P R_X [Z] C PR_y [Z]) A (P R_X[T] = PR_y [T)]) subcase(b): (P R_X[Z] = PR_y [Z]) A (P R_X [T] ¹ PR_y [T]) subcase(c): (P R_X [Z] C PR_y [Z]) A (P R_X[T] ¹ PR_y [T]) subcase(d): (P R_X[Z] = PR_y [Z]) A (P R_X [T] = PR_y [T])

To resolve the conflicts from a global policy model, we introduce the concept of rule-order majority. For example, considering a pair of conflicting rules PR_X and PR_y . PR_X has higher relative order than PR_y iff x < y; where the suffix indicate the relative rule index (positions) in the rule base. Thus for each such pair of rules, we state PR_X as order-major and PR_y as order-minor rule.
Now, in all the subcases under Case 2 and subcase 1(d), resolving the inter-rule conflicts require deletion of the order-minor rules, PR_y . Whereas, in subcase 1(a), rule PR_X must be replaced by the rule

$PR^{!x}$ keeping PR_y unchanged where

$PR^{!x}$:< PR_X[role], (P R_X[Z] − PR_y [Z]), PR_X [obj], PR_X [T], PR_X[p] >.
Similarly, in subcase 1(b), the rule PR_X must be replaced by the rule $PR^{!!x}$, where $_x^{PR}$:< PR_X[role], (P R_X [Z] − PR_y [Z]), R_X[obj], (P R_X[T] − PR_y [T]), PR_X[p] >.

The global policy rule base generated after the removal of the inter-rule conflicts is repre-sented as GP .

High Level Policy Configuration: To enforce the organisational security policy in the wireless LAN, the rules in the conflict-free global policy model GP must be properly dis- tributed to various policy zone controllers (WPZCon). Thus, GP is represented as a distri- bution of zonal rule sets < GP_{Z_1} , GP_{Z_2} , ..., GP_{Z_N} >, where GP_{Z_i} represents the zonal rule set for the policy zone Z_i. To make this distribution correct, the following property must be satisfied: $(GP_{Z_1} \; A\, GP_{Z_2} \; A \ldots A\, GP_{Z_N}) \Rightarrow GP$. A policy rule PR_i is included in the zonal rule set GP_{Z_k} corresponding to the policy zone Z_k , iff the policy zone of PR_i is contained by the policy zone Z_k . This is formally represented as follows: $\forall PR_i \in GP, \exists Z_k \; c\, Any, (Z_k \; c\, PR_i[Z] \Rightarrow (PR_i[Z] \Uparrow GP_{Z_k}))$. Here, $(PR_i \Uparrow GP_{Z_k})$ indicates the inclusion of PR_i in GP_{Z_k} . Thus, $\forall k, GP_{Z_k} \; c\, GP$. In our model, < GP_{Z_1} , GP_{Z_2} , ..., GP_{Z_N} > represents the high level policy configuration corresponding to the global policy GP .

Low Level Access Configuration: The global policy server (GPS) distributes the zonal rule sets of the high level policy configuration to various policy zone controllers (WPZCon). Each WPZCon translates the zonal rule set to low level configuration based on the local policy zone information. A WPZCon coordinates with the local role server (LRS) and access points (AP) for getting populated with the local policy states. The low level access configuration LP_{Z_k} represents a collection of implementation rules $\{IR_1, IR_2, ..., IR_N\}$ corresponding to the zonal rule set GP_{Z_k} of policy zone Z_k .

Definition 6: [Implementation Rule] *An Implementation rule* IR_X $<u_i, r_j, Serv_k, Z_s, Z_d, T, p, net_l>$ *defines that an user* u_i *associated to the role* r_j *is assigned the permission* p *to access the network service* $Serv_k$ *from the source zone* Z_s *to destination zone* Z_d *during time interval* T; where, net_l *represents the access router or the network interface to which the rule is phys- ically mapped.*

For each implementation rule, IR_i, the service $Serv_k$ and destination policy zone Z_d can be determined from the associated network object $(PR_i[Obj])$ corresponding to the policy rule PR_i . More importantly, the relation $UserRoleAssign(u_i, r_j, T, Z_k)$ [described in section 4.3] ensures the correct user-role mapping which satisfies the following property:

$UserRoleAssign(u_i, r_j, T, Z_k) \Rightarrow (UserPZone(u_i, T) = Z_k) A$
$(Z_k \; c\, RoleAssignZon(r_j)) \; A \, (T \; c\, RoleAssignTime(r_j))$.

The validation of the low level access configuration is ensured by the property: $\forall (LP_{Z_i}, GP_{Z_i}), LP_{Z_i} \Rightarrow GP_{Z_i}$. It states that each low level implementation rule set or access configuration, LP_{Z_i} must conform to the corresponding high level policy rule set GP_{Z_i}

5. STRBAC Model Analysis with case study

In this work, we propose a WLAN policy management system supported by a spatio-temporal RBAC model. In this section, we analyze the framework with a case study. We consider a typical *Academic WLAN* conforming to Fig 1 with a global policy *Example policy*. The network consists of four wireless policy zones, namely *Hall* [refers to student hall of residences], *Academic*[refers to academic departments], *Administration* [refers to administrative block] and *Web Proxy* [refers to the policy zone consisting of web-proxy servers]. The *internet(http)* access to the external world is processed through *Web Proxy* zone. *Example policy:*

- The Academic network consists of five roles: *student, faculty, administrative staff, network administrator* and *guest*.
- The network services considered: *ssh, telnet* and *http* conforms to TCP/IP protocol.
- The *network administrator* can *always* access *internet* from *any* zone and can *always* access *ssh* and *telnet* from *any* zone to *any* zone.
- *faculty* can always access *internet* from *any* zone and can always access *ssh* and *telnet* from *any* zone to only *Academic* zone.
- *administrative staffs* can always access *internet* from *any* zone and can always access *ssh* and *telnet* from *any* zone to only *Administration* zone.
- *students* can not access *internet* from the *Hall* zone during *working hours*, i.e., *08:00-18:00, Monday to Friday*
- *students* can *always* access *internet* from *Academic* zone and can *always* access *ssh* and *telnet* only from *Academic* zone to the same zone.
- *guests* can access *internet* only from *Academic* zone during *working hours*.

Example:STRBAC Model [STRBAC model for Example policy:]

1. Policy Zones = {Hall, Academic, Admin, Web_Proxy}
2. Network Objects = {O1<ssh,Academic>, O2<ssh,Admin>, O3<ssh,Any>,
   O4<telnet,Academic>, O5<telnet,Admin>, O6<telnet,Any>,
   O7<http,Web_Proxy>}
3. Working hours(WH) = (2,3,4,5,6).Day@(<8.hr+00.min>:<17.hr+59.min>)
4. Always = (1,2,3,4,5,6,7).Day@(<01.hr+00.min>:<23.hr+59.min>)
5. Non-working hours(NWH) = {(2,3,4,5,6).Day@(<1.hr+00.min>:<7.hr+59.min>),
   (2,3,4,5,6).Day@(<18.hr+00.min>:<23.hr+59.min>),
   (1,7).Day@(<1.hr+00.min>:<23.hr+59.min>
)}
6. Roles = {r1<student>, r2<faculty>, r3<administrative
   staff>, r4<network administrator>, r5<guest>}
7. RoleAssign
   ={(r1,<Hall,NWH>,<Academic,WH>),(r2,Any,Always),
   (r3,Any,Always), (r4,Any,Always),(r5,Academic,WH)}
8. Users = {user1,user2,user3,user4,user5}
9. Global Policy(GP) ={PR1<r4,Any,O7,Always,permit>,
   PR2<r4,Any,O3,Always,permit>, PR3<r4,Any,O6,Always,permit>,
   PR4<r2,Any,O1,Always,permit>, PR5<r2,Any,O4,Always,permit>,
   PR6<r2,Any,O7,Always,permit>, PR7<r3,Any,O2,Always,permit>,

PR8<r3,Any,O5,Always,permit>, PR9<r3,Any,O7,Always,permit>,
PR10<r1,Academic,O1,Always,permit>,
PR11<r1,Academic,O4,Always,permit>, PR12<r1,Hall,O7,NWH ,permit>,
PR13<r1,Hall,O7,WH,deny>, PR14<r1,Academic,O7,Always,permit>,
PR15<r5,Academic,O7,WH,permit>}

10. User-Role Assignment = {(user1,r1), (user2,r2), (user3,r3), (user4,r4)}
11. High level policy config = (GP_{Hall}{PR1,PR2,..,PR9,PR12,PR13}, $GP_{Academic}${PR1,..,PR9,PR10,PR11,PR14,PR15}, GP_{Admin}{PR1,..,PR9})
12. Low level access config corresponding to policy zone Hall(LP_{Hall}) =
{IR1<user4,r4,http,Any,Web_Proxy,Always,permit,net_1>,
IR2<user4,r4,ssh,Any,Any,Always,permit,net_1>,...,
IR9<user3,r3,http,Any,Web_Proxy,Always,permit,net_1}>,
IR10<user1,r1,http,Hall,Web_Proxy,NWH ,permit,net_1>,
IR11<user1,r1,http,Hall,Web_Proxy,WH ,deny,net_1>}.

Property Validation:

Property1: $UserRoleAssign(u_i, r_j, T, Z_k) \Rightarrow (UserPZone(u_i, T) = Z_k)\ A\ (Z_k \subset RoleAssignZon(r_j))\ A\ (T \subset RoleAssignTime(r_j))$.

Property2*:* $GP_{H\ all}\ A\ GP_{Academic}\ A\ GP_{Admin} \Rightarrow GP$.

Property3*:* $((LP_{H\ all} \Rightarrow GP_{H\ all})\ A\ (LP_{Academic}\ A \Rightarrow GP_{Academic})\ A\ (LP_{Admin} \Rightarrow GP_{Admin}))$.

The *Example STRBAC* represents the model corresponding to *Example policy* in the academic network. Here, the model shows the low level access configuration corresponding to Hallzone. Similarly, the configurations for other policy zones are derived. Although the example considers one user corresponds to one role, multiple users can be assigned to one role also. The security of the proposed STRBAC model is ensured by *Property1*, *Property2* and *Property3*. The SAT based verification procedure for checking the satisfiability of the properties has been described in the next section.

We have shown, how the global policy of an organizational WLAN can be formally modeled using STRBAC and then described the hierarchical formulation of the high level and low level configurations. The model supports the proposed policy management system archi- tecture. The proposed system is scalable as the task of policy configurations and validations are managed in a distributed manner.

6. SECURITY PROPERTY VERIFICATION WITH SAT BASED APPROACH

In SAT based approach, the verification problem is reduced into boolean formula and its satisfiability is checked. Although satisfiability analysis is NP complete problem, still this technique is becoming popular today due to tremendous time tradeoffs of modern SAT [14] and QBF-SAT solvers [13]. In the present work, the STRBAC model, Global policy (GP), high level policy configurations ($< GP_{Z_1}, GP_{Z_2}, ..., GP_{Z_N} >$) and the low level access con- figurations ($< LP_{Z_1}, ..., LP_{Z_N} >$) are reduced into set of boolean clauses. Then the desired security properties, i.e., *Property1*, *Property2* and *Property3* [described in section 5] are re- duced into boolean clauses which are fed as SAT query to the SAT solver [14]. The SAT solver checks the satisfiability of the properties to assess the access configuration with respect to the global policy.

6.1 Boolean Modeling STRBAC Entities

In this section, the boolean reduction of STRBAC entities related to our system has been described. The entities in our model includes *users, roles, time, source* and *destination policy zones* and *network services*. Here a *network service* and a *destination policy zone* compositely define a *network object*.

Each *user or host* is identified by a MAC address which is a 48 bit number. So, *users* are modeled as 48 boolean variables, namely, (u_0, u_1, ..., u_{47}). Similarly, *roles* are modeled as 4 boolean variables, namely, (r_0, r_1, ..., r_3) where we consider 16 different roles. The *source* and *destination* policy zones are represented as collection of IP addresses. So, we model the *source* and *destination* policy zones with 32 boolean variables each, namely, (s_0, s_1, ..., s_{31}) and (d_0, d_1, ..., d_{31}) respectively. A range of IP addresses can be translated using disjunction ($\vee$) operator. Address ranges with masks can be reduced by bit-wise anding the masks with the base addresses. Similarly, protocol type and service port numbers are mapped into 5 and 16 boolean variables, namely, (p_0, p_1, ..., p_4) and (i_0, i_1, ..., i_{15}) considering 32 different protocols and 65356 different service ports respectively. A *network service* is modeled as conjunction (A) between a protocol and a service port number. A *network object* is modeled as conjunction (A) between a service and a destination policy zone. *Time* constraints are modeled as disjunction of its valid periods. Each valid time period can contain *day of week*, *hours* and *minutes* etc. The components of a valid time period are mapped mapped into a set of boolean variables, namely, (dt_0, dt_1, dt_2), (th_0, th_1, ..., th_4) and (tm_0, tm_1, ..., tm_5) respectively. Here we have considered the granularity of time in minute. The mapping of STRBAC entities into boolean variables is presented in table 1.

The $UserPZone$, $RoleAssignTime$, $RoleAssignZone$ and $UserRoleAssign$ functions are modeled through four boolean functions, namely $FUZone(u_i, T_i, Z_i)$, $FRATime(r_i, T_i, Z_i)$, $FRAZone(r_i, Z_i, T_i)$ and (u_i, r_i, T_i, Z_i) which are also presented in table 1.

Table 1: Boolean mapping of the STRBAC entities & Functions

Users/Hosts/macid(u):FUmac($u_0, u_1, ..., u_{47}$)

Roles(r):FR($r_0, r_1, ..., r_3$)

Protocol(P):FP($p_0, p_1, .., p_4$)

Service_PortNo(I):FI($i_0, i_1, ..., i_{15}$)

Src_zone_IP(SIP):FSZ($s_0, s_1, ..., s_{31}$)

Dst_zone_IP(DIP):FDZ($d_0, d_1, ..., d_{31}$)

Zone_Access_Router_IP(ARIP):FZAP($s_0, s_1, ..., s_{31}$)

Time(T):FTIME($dt_0, dt_1, dt_2, th_0, .., th_4, tm_0, tm_1, ..., tm_5$)

Action(g):$A(g)$

UserPZone(u,T):FUZone(u_i, T_i) $\Rightarrow Z_i$

RoleAssignTime(r,T,Z):FRATime(r_i, T_i) $\Rightarrow Z_i$

RoleAssignZone(r,Z,T):FRATime(r_i, Z_i) $\Rightarrow T_i$

UserRoleAssign(u,r,T,Z):FURA(u_i, r_i, T_i, Z_i)

6.2 Boolean Modelling of Policy and Access Configurations

This section describes the boolean reduction of policy and low level access configurations. In both the models, the rule components are same except the network *access router* (or wireless policy zone interface) information in the low level access configuration. As access router IP address corresponding to a policy zone contained in the zone IP address block, it is modeled through same set of boolean variables as source policy zone, namely, (s_0, s_1, ..., s_{31}). The following sections describes the reduction of the policy and low level access configurations.

6.2.1 Reduction of Global Policy and High level Policy Configurations:

Global policy is represented as collection of policy rules with following components: roles, source-policy zone, network object and permissions. The global policy (GP) is reduced into two boolean functions, "permit"(P T gp) and "deny"(P F gp) where each function incorporates corresponding "permit" and "deny" rules through disjunction(∨) operator. The formulation is described as follows:
P Ri ⇔ (F Ri A SI Pi A Obji A Ti A Ai); where Obji ⇔ (Pi A Ii A DI Pi)
P T gp ⇔ (, P Rj) VP Rj (action) = "permit"
P F gp ⇔ (, P Rk) VP Rk (action) = "deny"
Similarly, the high level policy configuration is represented as collection of zone-wise policy rule sets and hence reduced to two boolean functions for each zone ZX, namely, P T Zx and P F Zx respectively. The formulation is described as follows:
P T Zx ⇔ (, P Rj) VP Rj (action) = "permit" AP Rj (SI Pj) = ZX
P F Zx ⇔ (, P Rj) VP Rj (action) = "deny" AP Rj (SI Pj) = ZX
In this way, the global policy and high-level policy configurations are reduced into boolean clauses.

6.2.2 Reduction of Low level Access Configurations:

Low level access configuration is represented as zone wise distribution of low level access rules (I R). Each low level access rule contains the following components; user, role, network service, source policy zone, destination policy zone, time constraints, permission and access router (or wireless policy zone interface) IP address. In our model, the access router IP is considered as the first IP address in the corresponding wireless zone IP block. The low level access configuration for each policy zone ZX is reduced into two boolean functions LAT Zx and LAF Zx . The formulation of low level access rules and zone-wise access configurations are described as follows:
I Ri ⇔ (ui A ri A SI Pi A DI Pi A Ti A Ai A ARI Pi) where, ARI Pi ⊕ SI Pi = 000..01;
LAT Zx ⇔ (, I Rj) VI Rj (action) = "permit"
LAF Zx ⇔ (, I Rj) VI Rj (action) = "deny" AI Rj (SI Pj) = ZX In this way the low level access rules and the access configurations are reduced into boolean clauses.

6.3 SAT Solver and SAT Query Formulation

We have modeled our verification problem to SAT Query which can be verified through zChaff SAT solver [14] tool. It takes SAT query in conjunctive normal form (CNF) and checks its satisfiability. The commonly used format for storing CNF formulae in ASCII files is DIMACS [15].
SAT query for the present problem is conjunction of Property1, Property2 and Propwerty3 described in section 5. So, it is sufficient to check the satisfiability of the following expressions: F = P r1 A P r2 A P r3 where,

P r1 ⇔ [U serRoleAssign(ui , rj , T , Zk) ⇒ (U serP Z one(ui , T) = Zk)A(Zk c RoleAssignZ on(rj))A
(T c RoleAssignT ime(rj))];
P r2 ⇔ [GPH all A GPAcademic A GPAdmin ⇒ GP] and
P r3 ⇔ [((LPH all ⇒ GPH all) A (LPAcademic A ⇒ GPAcademic)A (LPAdmin ⇒ GPAdmin))]

In our framework, the formula F is translated into CNF using standard algorithm for 3-CNF satisfiability [12]. The algorithm forms truth tables for every sub-expression containing disjunctions of conjunctions and converts it into CNF applying De-Morgan's rules where each clause contains at most 3 literals. For example, equivalent CNF for the the formula P r2 ⇔ [GPH all A GPAcademic A GPAdmin ⇒ GP] can be represented as (¬P r2 ∨ ¬GPH all ∨
¬GPAcademic ∨ ¬GPAdmin) A (P r2 ∨ GPH all) A (P r2 ∨ GPAcademic) A (P r2 ∨ GPAdmin) A (P r3 ∨ ¬GP). The formula F (in DIMACS CNF format) is provided as input to zChaff. It checks
the SAT or UNSAT of the formula. Here, the SAT result implies that the the low level access configuration conforms to global policy and the high level policy configuration whereas UNSAT result indicates that the low level access configuration is incorrect. In that case the unsatisfiable instance indicates the violating rule.

7. RESULTS AND DISCUSSIONS

To ensure the correctness of the proposed STRBAC model in the WLAN security management system, we have used SAT based verification procedure. The verification procedure has been implemented in C programming language under Linux environment. The framework has been tested with various policy configurations in an enterprise wireless network.

The table 2 shows experimental results of verifying different policy configurations under the network.

Table 2 shows number of policy rules in the global security policy specification, number of Boolean clauses in the SAT query, number of conflicts detected in the model, property verification result (SAT/UNSAT) along with timing parameters. The parameters #P , #C N F and #C indicate the number of policy rules, number of boolean (CNF) clauses in the SAT query and number of conflicts detected in the global policy specification respectively. The output indicates the property verification result from the zChaff SAT solver [14]. The result reports SAT only if all the properties are satisfied by the model. Whereas, UNSAT result indicates the violation of the security properties with violating instance. For example, in both the UNSAT test cases (refer table 2), the Property3 is violated. This indicates the low level access configurations do not conform to the high level policy configurations. In such cases, the derived low level access configurations must be reconfigured by modifying imple- mentation rules accordingly. The TSAT and TeXec represent the SAT reduction and zChaff execution time respectively. The SAT reduction time is linearly dependent on the number of policy rules whereas the zChaff execution time is dependent on the internal evaluation of the SAT query which is almost constant in the order of milliseconds. The number of policy rules for large scale enterprise network usually lies within a few hundreds. So, the framework is scalable.

Table 2: Property Verification Results with Timing Analysis

$\#P$	$\#CNF$	$\#C$	Output	T_{SAT} (sec)	T_{eXec} (sec)
15	402	0	SAT	3.34	0.018
25	553	1	SAT	4.25	0.032
53	578	0	UNSAT	6.72	0.025
64	785	2	SAT	7.84	0.036
70	918	1	SAT	8.44	0.025
95	1485	0	UNSAT	10.46	0.022
115	1740	3	SAT	12.51	0.033

Moreover, the use of distributed policy zone controllers (WPZCon) makes the task of policy enforcement and validation easier and efficient. The proposed framework may help the network administrator for debugging the security policy configurations for large scale enterprise WLAN.

8. CONCLUSION

In this paper we present a security policy management system for Wireless Network (WLAN) supported by a formal spatio-temporal RBAC model compatible with mobile IP. The use of mobile IP to wireless nodes ensures that the node IP does not change with mobility. The global security policy of the enterprise is enforced through distributed wireless policy zone controllers (WPZCons) which are populated by extracting the high level policy configurations from the global policy server (GPS). This makes policy enforcement and validation simple and efficient. We present a spatio-temporal RBAC model to support the policy management system which ensures the time and location dependent access to the network objects and hence provides strong security perimeter over an organizational WLAN. We have also present a SAT based verification framework for checking the correct enforcement of the access policies in the wireless access routers.

REFERENCES

[1] Basile, C., Lioy, A., Prez, G. M., Clemente, F. J. G. and Skarmeta, A. F. G. 'POSITIF: a policy-based security management system', *In 8th IEEE International Workshop on Policies for Distributed Systems and Networks (POLICY07)*, pp. 280–280, Bologna, Italy, June 2007.

[2] Lapiotis, G., Kim, B., Das, S. and Anjum, F. 'A Policy-based Approach to Wireless LAN Se- curity Management', *In International Workshop on Security and Privacy for Emerging Areas in Communication Networks*, pp.181–189, Athens, Greece, September 2005.

[3] Burns, J., Cheng, A., Gurung, P., Rajagopalan, S., Rao, P., Rosenbluth,D. and Martin, D. 'Automatic Mnagement of Network Security Policy', *Proceedings of the 2nd DARPA Information Survivability Conference and Exposition (DISCEX II)* pp.12–26, Anaheim, California, June 2001.

[4] Yavatkar, R., Pendarakis, D. and Guerin, R. 'RFC 2753: A Framework for Policy-based Admission Control', *Internet Society*, pp.1–20, January 2000.

[5] Westrinen, A., Schnizlein, J., Strassner, J., Scherling, M., Quinn, B., Herzog, S., Carlson, M., Perry, J. and Wldbusser, S. 'RFC 3198: Terminology for Policy-Based Management', *Internet Society*, pp.1–21, November 2001.

[6] Ferraiolo, D. F., Sandhu, R., Gavrila, S., Kuhn, D. R. and Chandramouli, R. 'Proposed NIST standard for Role-Based Access Control', *ACM Transactions on Information and Systems Security*, vol. 4(3), August 2001.

[7] Joshi, J. B. D., Bertino, E., Latif, U., and Ghafoor, A. 'A Generalized Temporal Role-Based Access Control Model', *IEEE Transactions on Knowledge and Data Engineering*, vol.17(1), pp.4–23, 2005.

[8] Bertino, E., Catania, B., Damiani, M. L. and Perlasca, P. 'GEO-RBAC: a spatially aware RBAC', *In SACMAT05:Proceedings of the tenth ACM symposium on Access control models and technolo- gies*, pp.29–37, NY, USA, 2005.

[9] Ray, I., and Toahchoodee, M. 'A Spatio-Temporal Role-Based Access Control Model', *In DBSec2007, Data and Application Security*, Lecture Notes in Computer Science, vol.4602, pp.211–226, 2007.

[10] Tomur, E., and Erten, Y. M. 'Application of Temporal and Spatial role based access control in 802.11 wireless networks', *In the Journal of Computers & Security*, vol.25, issue 6, pp.452–458, September 2006.

[11] Laborde, R., Nasser, B., Grasset, F., Barrere, F. Benzekri, A. 'A Formal Approach for the Eval- uation of Network Security Mechanisms Based on RBAC policies', *Electronic Notes in Theoritical Computer Science*, vol.121, pp.117–142, February 2005.

[12] T. Hofmeister, U. Schoning, R. Schuler, and O. Watanabe. 'A Probabilistic 3-SAT Algorithm fur- ther improved.' *19th Annual Symposium on Theoritical Aspects of Computer Science (SATACS)*, LNCS 2285, pp. 192-202 Springer-Verlag, 2002.

[13] L. Zhang and S. Malik. 'Towards Symmetric treatment of Conflicts and satisfaction in quantified Boolean satisfiability.' *In Principles and Practice of Constraint Programming (CP 2002)*, pp. 185-199, 2002.

[14] Y. S. Mahajan, Z. Fu, and S. Malik. 'Zchaff 2004: An efficient SAT solver.' *In Proceedings of 8th International Conference on Theory and Application of Satisfiability Testing*, LNCS 3542, pp. 360-375, Scotland, June 2005.

[15] O. Dubois, P. Andre, Y. Boufkhad, and J. Carlier. 'SAT versus UNSAT, Second DIMACS chal- lenge.' *D.S. Johnson and M.A. Trick Eds,* 1993.

[16] Bhagyavati, W. C. Summers and A. Dejoie. 'Wireless security techniques: an overview' *In Proceedings of 1st International Conference on Information Security curriculum development (In- foSecCD04)*, pp. 82-87, Kennesaw, Georgia, 2004, ACM Press, NY, USA.

[17] RFC4721, Internet Engineering Task Force, 2007

[18] P. Bera , S. K. Ghosh and Pallab Dasgupta 'A Spatio-Temporal Role-Based Access Control Model for Wireless LAN Security Policy Management' *Information Systems, Technology and Manage- ment, 4th International Conference, ICISTM 2010, Bangkok, Thailand, March,2010. Proceedings*

[19] Perkins, C.E. 'Mobile ip', *International Journal of Communication Systems, volum 11, num- ber 1,pages 3–20,1998,John Wiley & Sons*

[20] Padmalochan Bera, Pallab Dasgupta, S. K. Ghosh 'Formal Analysis of Security Policy Implemen- tations in Enterprise Networks', *International Journal of Computer Networks & Communications (IJCNC), Vol 2(2), pp 56-73, July 2009*

Soumya Maity

Soumya Maity is pursuing PhD from Indian Institute of Technology, Kharagpur under the supervision of Dr. S. K Ghosh. He has joined as a PhD student in 2008 directly after his B.Tech in Computer Science and Engineering from West Bengal University of Technology, Kolkata, India in the same year. Wireless Networks,Information Security and Embedded Systems are his domain of interest.

P. Bera

P Bera is a PhD student in School of Information Technology at Indian Institute of Technology, Kharagpur, working under the supervision of Dr. S. K. Ghosh and Dr. Pallab Dasgupta. He received BE and ME in Computer Science & Engineering respectively from Jadavpur University and West Bengal University of Technology, Kolkata, India. His current research area is Network and Information Systems Security. He has good number of research publications in reputed conferences and journals. His other research interests include Formal Property Verification, Distributed Systems and Access Control Models.

Dr. S. K. Ghosh

Dr. S K Ghosh did his M.Tech and PhD in Computer Science & Engineering from the Indian Institute of Technology (IIT) Kharagpur,India. He is currently an Associate Professor at the School of Information Technology, IIT Kharagpur. Before joining IIT Kharagpur,Dr. Ghosh worked for Indian Space Research Organization in the area of Satellite Remote Sensing and GIS. His research interests include Network Security and Spatial Web Services. He has over 50 research papers in reputed conferences and journals. He is a member of IEEE.

Dr. Pallab Dasgupta

Dr. Pallab Dasgupta did his B.Tech, M.Tech and PhD in Computer Science from the Indian Institute of Technology Kharagpur. He is currently a Professor at the Department of Computer Science and Engineering, Indian Institute of Technology Kharagpur. His research interests include Formal Verification, Artificial Intelligence and VLSI. He has over 100 research papers and 2 books in these areas. He currently leads the Formal Verification group at the CSE Dept, IIT Kharagpur which has been developing validation technology for several companies, including Intel, Synopsys, General Motors, SRC and National semiconductors.Since Oct 2007, he is also the Professor-in-charge of the Advanced VLSI Design Lab, IIT Kharagpur. Dr. Dasgupta has been a recipient of the Young Scientist awards from the Indian National Science Academy, Indian National Academy of Engineering, and the Indian Academy of Science. He is a senior member of IEEE