International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 5
May 2017

Adaptive Security Architecture for Physical layer security in Wireless Networks

Varad A. Sarve
SGBAU, Amravati,
Maharashtra, India.

Dr. Swati S. Sherekar
SGBAU, Amravati,
Maharashtra, India.

Dr. Vilas M. Thakare
SGBAU, Amravati,
Maharashtra, India.

Abstract—Wireless networks are predominantlyused as major network scenario these days. While many security methods has been deployed, physical layer security should be considered as primary security issue for the growing mobile networks.Users are more aware of their privacy and consent about any violation of protocols of the network.Anonymity and Traceability are the important constraints for wireless networks which are potentially more susceptible to security vulnerabilities. The seamless provision of services over the network also needs some attention towards security at the physical layer as it is first preference of the eavesdropper to get valuable information. This paper presents an Adaptive Security Algorithm (ASA) that caters as security essential in distributed wireless network. Source-destination pair is assisted by a friendly jammer to enforce security against misbehavior in the network. Proposed algorithm also focuses on Channel State Information's (CSI) availability, perfectly known or statistically known, for adaption of one of security method. Security methods based on CSI includes, generation of interference, secrecy rate maximization and limiting knowledge of existence of information from eavesdropper. Finally, beamforming transmission strategy is used to employ reliable transmission, reduction of exposure region over distributed environment.

Index Terms—Physical Layer Security, cooperative jamming, secrecy rate maximization, Anonymity, Traceability.

I. INTRODUCTION

Wireless Networks plays major role in broadband services in today's world with increasing number of user friendly features such as privacy and security. Wireless Radio links are another important element where cable-based alternatives are required. Mobile cloud is dominant technology in providing computing resources and infrastructure to support seamless provision of network services [1] [2] [3]. However, these attractive features also bring in many issues related to the security before deployment. Anonymity is used by misbehaving entities in the network. Anonymity and privacy issues have gained considerableresearch efforts which havefocused on investigating anonymity in different context or application scenarios.Traceability for such users is necessary to provide security for valuable information [1]. Radio linksare not that secure as channel information may easily expose the valuable information to adversaries. Prior security threat analysis can be useful to secure the radio channel [2]. Mobile cloud security is also a major issue for advance development in mobile networks such as 3G/4G. The functionality of the cloud is based on distributed management and task distribution mechanisms. The technology of this distributed service implementation is based on representational state transfer (REST) design principles. Security functionalities are also considered as robust for complex mobile web service provisioning [3].One way to keep such misbehaviors under control is to assist nodes in the network with jamming nodes which can be used as shield against eavesdropper. This is achieved by a friendly jammer transmitting a jamming power signal, which has the effect of decreasing the signal-to-noise ratio at the eavesdropper, referred to as *cooperative jamming*[4]. Another approach to model security between users is a scheme where transmission adapts strategy according to the channel state information of the eavesdropper.A cooperative transmission scheme is provided for secrecy rate maximization, subject to both security and quality of service constraints. Secrecy rate can also be maximized to obtained efficient usages of network resources and confidentiality between sender-receiver nodes [5]. Smart Antennas are fine example of the secure communications over wireless data networks. These antennas not only hide the meaning of the information being sent (cryptography) but also limit the knowledge of existence in the first place. Eavesdropper can only

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 5
May 2017

explore part of the message under exposure region which can be reduced exponentially to limit the decoding of the signals. Smart antennas are used in association with cooperative jamming and transmission scheme for better security in the network [6].

In this paper, Security architecture is explained for different parameter of both network and network users. Objectives for security and assets required in it to identify the potential security threats are also explored. While keeping user identity hidden, misbehaving users are exposed and restricted in future to have network services. Requirements for resources and infrastructure of the network are configured with appropriate authentication and confidentiality using existing security protocol in association with some new security goals. Physical layer security is the main focus of this paper. Environments such as, 2-cell, distributed and mesh network are considered to give the proposed algorithm a wide range of application. Algorithm binds friendly jammers with source nodes which require protection from eavesdropper. A flexible securitymethod uses matching, channel state information and beamforming for the nodes.

II. BACKGROUND

All the entities in the wireless network are generally operated by a central administrative entity, which is also responsible for providing security services and privacy for the users. Anonymity for the users as well as traceability for misbehaving users is some of the greedy features of the new generation mobile networks. A security analysis, list of basic assumptions, security objectives are proposed in [1]. Securityarchitecture to resolve the conflicts between the anonymity and traceability objectives is proposed in [2] to guarantee fundamental security requirements including authentication, confidentiality.Major contributions in thisinclude design of a ticket-based anonymity system with traceability property. Tickets are allocated to the users to enable their access based on the misbehaving history and in this way anonymity can be achieved as well as traceability can be implemented without disclosure of the identity of the users. A security framework is presented in [3] to provide authentication and confidentiality between clients and mobile hosts using mobile cloud services. The security for every component is characterized and security aspects for complex web services are investigated. A prototype is implemented for this framework in order to provide seamless provision of web services. A distributed algorithmthat matches each source-destination pair with a particular jammer is given in [4]. A utility-based matching framework is proposed to motivate multiple source nodes and multiple friendly jammers to cooperate with each other such that the sum-secrecy rate over all source nodes is maximized.All nodes calculate the jamming power requirement and get associated with jammers accordingly. A framework of physical layer security in networks through adaptive base station cooperation is presented in [5] which provide an adaptable transmission scheme. The channel state information of the eavesdropper plays an important role in deciding the transmission scheme. Finally, a smart antenna, an example of securing communication over wireless data networks is proposed in [6]. It considers strategies that limit knowledge of the existence of the information from the eavesdropper. Advantage in this scenario is, eavesdropper can only be able to read data from exposure region and can be limited in that also. All these strategies to secure physical layer are merged together to provide security without compromising network security rules.

This paper is organized as follows, Section I gives the brief description about the importance of Physical Layer Security and its methods as well as methods proposed in this paper. Section II gives basics about the related methodologies on security to be considered primitively.

III. PREVIOUS WORKDONE

Frank A. Zdarsky*et.al.* (2010) [1]proposed an analysis of 3G mobile network for security issues and devised a model which describes security objectives and assets to be protected. On this basis, potential security threats are analyzed with their respective risks. A set of security requirements is defined for the derived risk assessment. This basic model for security can be implemented using these risk assessments and security requirements.

Jinyuan Sun *et. al.*(2011) [2]proposed a security architecture which ensures both, anonymity for honest users and traceability for misbehaving users, by network authorities. Authentication, confidentiality, data integration are some fundamental security requirements which are ensured by proposed architecture resolving conflicts

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 5
May 2017

between anonymity and traceability. This is implemented by issuing a Ticket to every user for accessing network resources on the basis of user's history in the network. Proposed architecture is thorough analysis of security and efficiency as well as demonstrates feasibility and effectiveness of the network with it.

FedaAlshanwan*et. al.* (2015) [3] proposed a security framework for authentication and confidentiality between clients. Security aspects for every component are analyzed and existing security protocols are presented accordingly. This framework can encompasses given security model and be implemented with the association of framework given above. Resources and infrastructure for security framework are evaluated by a prototype implementation.

SiavashBayat*et. al.* (2013) [4] proposed a distributed algorithm for pairing source-destination with a friendly jammer which can be used as a protection against single eavesdropper. Calculation of jamming power requirement can encourage better optimal association between nodes and jammers. A stable matching can be improved to defend against the eavesdropper by convergence of secrecy rate of a centralized optimal solution.

Lin hu*et. al.* (2016) [5] proposed more advanced scenario to prevent unwanted eavesdropping where channel state information of the eavesdropper is known statistically and/or perfectly. The transmission scheme, configured for adaptation with security protection, can be termed as adaptive base station cooperation. This scheme also focused towards secrecy rate maximization using cooperative base station mechanism.

S. Lakshmanan*et. al.* (2010) [6] proposed a secure communication over wireless data network by using smart antennas. This antenna doesn't only hide the meaning of valuable information but its existence at all. Exposure region is the only place where eavesdropper can be effective, but strategies are implemented to limit this exposure region.

IV. EXISTING METHODOLOGY

A. Architecture of Anonymity and Traceability

Anonymity is achieved through ID-based cryptographywhich is derived by public identity of the user, based on public key cryptography. Participating nodes have to accept the message and the signature without knowledge of the sender. Encoded information is kept in message and restricted to the unintended users; trust domain is managed by a domain administrator that serves as a trusted authority (TA), e.g., the central server of a campus Wireless Mesh Networks. The client presents his ID upon registration at the TA, which assigns a private key associated with the client's ID. The client selects a unique account number Ω computed by a randomly chosen secret number u_1. The account number is stored with the client's ID at the TA. The TA also assigns an ID/private key pair to each gateway and mesh router in its trust domain before deployment [2].

Traceability is achieved through a Ticket-based security architecture which consists of ticket related functions for user tracking and detecting misbehaving in the network. Ticket insurance, Ticket deposit, Ticket revocation and fraud Detection are some of the functions which determine the user by its history of misbehaving [2].

The ticket generation algorithm, takes as input the client's and TA's secret numbers, the common agreement and some public parameters, and generates a valid ticket

$$ticket = \{T_N, W, c, (U', V', X', \rho, \sigma'_1, \sigma'_2)\}$$

at the output, where T_N is the unique serial number of the ticket, $(U', V', X', \rho, \sigma'_1, \sigma'_2)$ is the signature on

$$(T_N, W, c)$$

where$W$ is necessary for verifying the validity of the signature in the ticket deposit protocol.

B. Source nodes-Friendly jammer Matching Algorithm

SJMA obtains a solution to the optimization problem in distributed way; also secrecy rate is maximized according to the power requirement of the node. In exchange for providing jamming services to source, source will pay a monetary amount per jamming power to friendly jammer [4]. A utility functions evaluate the performance of each source node and jammer node. This function comprises the value of channel state information for the nodes taking part in the association of source-destination pair and friendly jammers. Jammers host the bids for the users and get bind with highest bidder. This association is useful in combating unwanted eavesdropping from an eavesdropper. Algorithm is implemented on distributed environment to match and maximize the secrecy rate over multiple iteration of the algorithm.

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 5
May 2017

A wireless network is considered comprising of;

N source node $\{S_l\}_{l=1}^{N}$ and destination node: $\{D_l\}_{l=1}^{N}$.

A set of M friendly jammers: $\{J_q\}_{q=1}^{M}$.

C. Adaptive Base Station Cooperative Scheme

A mechanism for transmit strategy adaptation with security protection is incorporated to provide security to a downlink transmission in two-cell wireless networks. Sender and Receiver can exchange messages with a cooperative base station to enhance secure transmission as well as they can share control signals and channel state information for cooperating services. Secrecy rate maximization is also an important issue in this scheme which can also be revised in matching algorithm. Channel state information can be useful to determine the cooperation scheme; it can be one of two, under perfect or static CSI [5].

Based on the notations and assumptions, the received signals can be expressed as

$$y_1 = H_{11}s_1 + H_{12}s_2 + n_1$$
$$y_e = h_{e1}^{H}s_1 + h_{e2}^{H}s_2 + n_e$$
$$y_2 = h_{21}^{H}s_1 + h_{22}^{H}s_2 + n_2$$

where$s_1$and $s_2$denote signals transmitted by Alice and Charlie, respectively; n_1, n_e, n_2 are mutually independent, and denote the additive complex white Gaussian noise (AWGN) at Bob, Eve and Rx2, respectively.

D. Smart Antennas for Physical Space security

To quantify the security achieved against eavesdropping in a wireless network, a new security metric is defined, called the *exposure region* of the network.This metric is where eavesdropper can derive information in the message and use it. To limit the knowledge of existence of the information in the message, smart antennas can be configured to beamform in physical and/or signal-space [6]. Another security element is to use virtual array of physical arrays. The architectural model used here consists of central access point which employs schemes above for stream of packets received from wireless LAN.

To quantify the security achieved against eavesdropping in a wireless network, define a new security metric called the *exposure region of the network*, ER_N, defined as the union of the exposure regions of all the clients in the network. The exposure region of the *i*th client, $ER(C_i)$, is given by the region in which an eavesdropper can decode the information of client *i*. Consequently

$$ER_N = \bigcup_{i=1}^{N_c} ER(C_i)$$

whereN_c is the total number of clients in the network.

E. Security Analysis and defensive methods

It is important to consider that a wireless mesh backhaul is supposed to provide a drop-in replacement for parts of the operator's wired backhaul. A 3rd Generation Partnership Project (3GPP) architecture provides its own security features, designed based on a separate security analysis. A traditional wireless access network focuses on the transport stratum. Transport between a user terminal (UT) and the core network distinguishes between the management and control plane which divides into the user signaling part between the UT and its Point of Attachment (PoA) and the core network signaling part between the network elements of the access network and the core network. The data plane transports data between the UT and the core network [1].

F. Security framework for resources and infrastructure

The purpose is to develop a secure mobile cloud infrastructure that facilitates continuous provisioning of complex mobile services. Complex services are defined as resource intensive and context-based services that are composed of multi-operations [3].

The performance for two different cloud structures has been investigated: one cloud supports security and the other does not. The application used for testing this scenario represents a simple mathematical service called PI Web Service, which used to calculate the constant π whose value can be approximated using the Gregory–Leibniz series:

$$\pi = 4 * \sum_{k=0}^{\infty} \frac{(-1)^k}{2k+1}$$

Different values of k are used to vary the computational intensity of the Web service sample. The amount of consumed power can be controlled via the k parameter. The bandwidth and processing demands can be controlled through this parameter.

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 5
May 2017

V. ANALYSIS AND DISCUSSION

In the Security architecture identification of nodes is main constraints to prevent the unwanted eavesdropping. Anonymity and Traceability provides this with the cost of ID based cryptography and ticket based authentication. Receivers have either to accept message without knowing the sender or trust the nodes authenticated by the trusted authority. But there is no way to know if sender is malicious node or trusted node. One way to manage the trusted entities is to allocate hierarchical based IDs which are inefficient in terms of computation and communication. Ticket based approach reduces communication overhead but introduces a constraints for clients to have minimal mobility during the usages of the deposited ticket [1].

Matching algorithm for source-destination pair and friendly jammers is an effective way of keeping eavesdropper busy with the complex distribution of messages. Jammers bind with any node that has calculated required jamming power and requested jamming services for the monetary price decided by the jammer.As jammers must broadcast the bidding information, so, case of jammers binding with nodes is also true for the eavesdropper who is ready to pay fair price for jamming services. The centralize method can be used to have this scenario under control with the cost of higher complexity and exponentially increased number of source nodes and jammers [2].

Cooperating base station or node, which is monitoring the messages with security protection, for single pair transmission is incorporated to implement an adaptive transmission scheme. Channel state information plays the major role for adaptation scheme decision, where it can be perfectly known or statistically known. In case of distributed network architecture this method is unable to provide security and eavesdropper can decode the jamming signal easily [3].

Information security can be efficiently handled if knowledge of its existence is limited. Smart antennas can perform this by beamforming and exposure region is exponentially reduced. But the network where many nodes are trying to communicate simultaneously beamforming introduces performance issues in terms of throughput. Distributed coordination also gets affected as security is unable to hold its importance as a primary objective [4].

Security Techniques	**Advantages**	**Disadvantages**
Architecture of Anonymity and Traceability	1) Security enables authentication at the access points and meets the access control security requirement. 2) Increases the communication efficiency by the avoidance of DPCs.	1) The basic HIDS can be very inefficient in terms of computation and communication. 2) Due to the limited ticket value, the client is expected to have minimal mobility during the usage of the deposited ticket.
Source nodes-Friendly jammer Matching Algorithm	1) Proposed SJMA can achieve a high percentage of the secrecy rate obtained by the centralized method. 2) The SJMA is distributed, and thus, incurs significantly less overhead and complexity compared to centralized algorithms.	1) The broadcast nature of the wireless transmission medium makes eavesdropping extremely easy. 2) Higher-layer security key distribution and management may be difficult to implement and may be vulnerable to attacks in some environments.
Adaptive Base Station Cooperative Scheme	1) Flexible and Environment-adaptive. 2) Efficient in Power Resource Utilization.	1) Only Single Antenna channel model is used. 2) Eavesdropper can decode jamming signal.
Smart Antennas for Physical Space security	1) Beamforming mechanism provides significant benefit over omnidirectional antennas using geometric models and simulations. 2) Virtual arrays of physical arrays significantly improve the exposure region performance of a wireless LAN environment.	1) Distributed coordination function is not considered in this approach. 2) Performance shifts between security to throughput.
Security Analysis and defensive methods	1) High Availability. 2) More Flexibility and efficiency.	1) More susceptible to security vulnerabilities. 2) Architectural design can compromise security goals.
Security framework for resources and infrastructure	1) Scalability and Generality. 2) Efficient networking functionality. 3) Supports HTTP protocol, Server Socket Connection.	1) Portability and the adverse effects of mobility on the connectivity of the devices limit the service quality on MHs.

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 5
May 2017

VI. PROPOSED METHODOLOGY

While using network services users often exposed to other users with some information for communication to be possible between two nodes in the network. Analysis of security threats becomes mandatorily important for devising security model for the network. Users may also want to limit each other from any sensitive information that may become potential to eavesdropping. Anonymity and privacy have focused on unlinking user's identity to his or her specific activities, which makes users to trust the network entities and applications. Malicious activities should also be traced and prevented by using ticket-based security architecture. By considering all these requirements for the security of the network, many authentication and confidentiality infrastructures and existing security protocols are arranged in a security framework.

The contribution in achieving security over distributed wireless network encapsulates physical layer security with friendly jammers and adaptive base station cooperation. Here, the proposed Adaptive Security Algorithm (ASA) is described to obtain a solution on secure transmission scheme using channel state information. Source nodes are primary attack place by eavesdropper where security is low for the transmission scheme compared to the link. The ASA consist of an initialization stage in step 1, followed by multiple iterations. In step 2, Source nodes calculate the required jamming power using utility function for security against eavesdropper. Once the power is calculated successfully it can then send this calculated value to the utility function of friendly jammer. Here, jammer can get request for jamming power from multiple nodes, hence, have to make a decision about the selection of node which will get jamming services. Machine learning can be used to effectively to learn about nodes behavior depending on its history. Jammer makes a price allocation offer to the source nodes requesting for the jamming power. Each node then determines the jammer which provides the highest positive utility. Jammers decision making is shown in step 3, where jammer can either increase the price allocation number to get maximum of the utility function or simply matched with the only request it have.

Once the matching is done, sender node is now able to transmit the message with interference to eavesdropper. Though there is enough level of interference, it is better to have the channel state information available for the purpose of securing the message itself with some security methods. In step 4 of the algorithm, Channel State Information (CSI) is checked for the transmit strategy adaptation with security protection. This can be either perfectly known or statistically known information. If it is statistically known, focused is tuned to secrecy rate maximization by applying beamforming transmission strategy. If CSI is perfectly known, which means every node is broadcasting its CSI over the network including eavesdropper. In this case, three different scenarios at the source nodes and jammers are considered, viz., 1) Global CSI, where jammers and source nodes have global instantaneous CSI. Jammers have knowledge of the CSI of the eavesdropper and CSI to destination node. 2) Local CSI, where source nodes has knowledge of the distribution of channels among nodes in the network. And 3) Local CSI without eavesdropper CSI, where local CSI of other nodes are known but any channel information regarding eavesdropper is not known.

In global CSI case, Jammers adjust their price allocation offer so that the interference created by it, will be maximum for the eavesdropper and minimum for the destination node. In local CSI case, we consider the complementary class of strategies that limit the knowledge of existence of the information from the eavesdropper. These three strategies are adopted in parallel for the security of physical layer in distributed wireless networks.

Algorithm takes two list types of structures for input namely as, Source nodes and available friendly jammers. Required power can be calculated using transmission properties such as, number of packets, size of packets, etc. When jammers price allocation offer is adjusted according to the request from source nodes, it can incorporate machine learning for learning about nodes and their behaving history using a database. Channel State Information contains properties of a communication link. This information describes how a signal propagates from the transmitter to the receiver and represents the combined effect of, scattering, fading and power decay and distance. Depending on the CSI, adoption of security constraints can be done. For statistic CSI, secrecy rate maximization is achieved by keeping anonymity of the user intact and providing information which is not potentially valuable. For

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 5
May 2017

perfect CSI, Interference generation for specific node i.e. malicious node is one of the finest ways for transmission through insecure medium in the presence of eavesdropper. Limiting knowledge of existence of information keeps eavesdropper away from the packets as they appear empty or useless to them. Distributed network is difficult to provide a constant communication links; Beamforming transmission scheme gives a reliable transmission and ensures the quality of the network strength.

ADAPTIVE SECURITY ALGORITHM (ASA)

Step 1: Initialization

(1) Construct the list of available friendly jammers.

Step 2: Source nodes calculates Required Jamming Power

(1) Jammers evaluates price allocation offer.

(2)Each source node determines jammer according to
it's requirement.

Step 3: Friendly jammer decision making

(1) If multiple source nodes requests jamming, increase
the price offer.

(2) Choose one which provides highest positive utility.

(3) If only one requests jamming, associate with it.

Step 4: Determine Channel State Information (CSI)

(1) Statistically known, Adopt secrecy rate maximization

(2) Perfectly known: Check for scope of CSI.

a. Global scope is eligible for enabling interference
on the network link.

b. Local scope, go to secrecy rate maximization.

c. Local scope without eavesdropper knowledge,
adopt limiting existence of knowledge.

Step 5: Transmission Scheme: Beamforming

Actual transmission of data in secure environment.

Step 6: End of the Algorithm.

Table I: Adaptive Security Algorithm (ASA)

Possible outcomes and result

The proposed approached is exponential overcome of the physical layer security as it is the primary level where attackers are more active rather than other parts of the network. As jammers assist source nodes, privacy of users is redeemed. Also, malicious nodes can also hide as a legitimate node if it pays fair allocation price. Thus, traceability is possible as jammers will have information about each node it provides jamming power services to. Matching of jammers with the source node gives source node protection against eavesdropping over distributed network environment. This scenario, unlike SJMA, is comparatively have low complexity and can work with more number of nodes than SJMA. Channel state information is used with great ease for deciding the security method which is effective over hierarchical as well as distributed network architecture. Finally, beamforming transmission scheme is advantageous for reliable communication for stable as well as mobile users. The problem of shifting focus between securities to throughput is also overcome as the history of misbehaving of node decides its position in the network hierarchy. Architectural design upholds security goals and security vulnerabilities are minimized. Even though broadcasting is necessary, it is no longer a potential for an attack.

VII. CONCLUSION

The objective of this security architecture has been to restrict potential security threats by minimum means necessary and to provide recommendations on how to resolve the underlying security issues for the cases that standard security solutions do not exist. The architecture also resolves the conflicting security requirements of unconditional anonymity for honest users and traceability of misbehaving users. A secure service framework is defined and shown that secure and private mobile cloud for providing jamming services is feasible and can enhance service performance and reliability in mobile network environments. The proposed algorithm converges to the optimal social welfare and a stable matching after a limited number of iterations. The proposition of the adaptive base station cooperation for beamforming with security protection is also contributed.

International Journal of Engineering Technology Science and Research
IJETSR
www.ijetsr.com
ISSN 2394 – 3386
Volume 4, Issue 5
May 2017

VIII. FUTURE SCOPE

This architecture restricts discussion to within the home domain which will be incorporated in future advancement. It would be interesting to consider the use of multiple antennas at the eavesdropper, source and destination nodes, extend the algorithm to cater for more than one jammer in the demand set and consider non-orthogonal source-destination channels. The secure transmission scheme will be further investigated for a more severe wiretap channel model, where the eavesdropper is equipped with multiple antennas. Further implementation also contributes to securing communication over wireless data networks and to a specific form of adversarial behavior-*eavesdropping*. Further, thesecurity threats targeted at the wireless access link (data and signaling), the core network (data and signaling) or the end-to-end user data protection will be covered. Constant service for varying structure of network will be a significant development over current framework. Also, this application can be scaled to more domains from the point of view of user centralized systems.

REFERENCES

[1] Frank A. Zdarsky, Sebastian Robitzsch, Albert Banchs, "Security analysis of wireless mesh backhauls for mobile networks", Journal of Network and Computer application, Vol. 34, No. 1, Pg. No. 432-442, April 2010.

[2] Jinyuan Sun, Chi Zhang, Yanchao Zhang, Yuguang Fang, "SAT: A Security Architecture achieving Anonymity and Traceability in Wireless Mesh Networks", IEEE transaction on Dependable and Secure Computing, Vol. 8, No. 2, Pg. No. 295-307, April 2011.

[3] FedaAlshahwanMaha Faisal Godwin Ansa, "Security framework for RESTful mobile cloud computing Web services", Journal of Intelligent Human Computing, DOI 10.1007/s12652-015-0308-5,August 2015.

[4] SiavashBayat, Raymond H. Y. Louie, Zhu Han, BrankaVucetic, Yonghui Li, "Physical-Layer Security in Distributed Wireless Networks using Matching Theory", IEEE transaction on Information Forensics and Security, Vol. 8, No. 5, Pg. No. 717-732, May 2013.

[5] Lin Hu, Hong Wen, Bin Wu, Fei Pan, "Adaptive Base Station Cooperation for Physical Layer Security in Two-Cell Wireless Networks", Journal of Security in Wireless Communication and Networking, 10.119/ACCESS.2016.2605918, September 2016.

[6] .SriranLakshmanan, Chen-Lin Tsao, RaghupathySivakumar, "Aegis: Physical Space Security for Wireless Networks with Smart Antennas", IEEE transaction on Networking, Vol. 18, No. 4, Pg. No. 1105-1118, August 2010.