iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** IV **Month of publication:** April 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Spontaneous Wireless ADHOC Network Creation, To Enhance Authentication Based On Self Configure Secure Protocol

N.Indumathi[1], D. Deva Hema[2]
M.Tech, Department of Computer Science and Engineering, SRM University, Ramapuram campus, Chennai-TamilNadu

Abstract —The proposal paper presents a self configured secure protocol for spontaneous wireless Adhoc networks which uses hybrid symmetric/ asymmetric scheme for encryption of the data. My proposal is to create a Spontaneous network with self configure secure protocol, to enhance the authentication during the communication over the network. The spontaneous network has without any infrastructure and central administrative. In spontaneous, when the nearby devices are interconnecting with each other, for short period of time and network is formed instantly without any infrastructure to exchange the information and to exchange the secret keys that will be used to encrypt data. The network will be created spontaneously for the completion of particular task that includes sharing resources with secure services. After completion of task the network will be disconnect from the network. In existing system of Adhoc wireless network plays to sharing of data with limited resources. In our proposal is to be creating a network for unlimited resources to join in the network, share the secure services for an authentication, and save energy of network without loss of packets.
Keywords: Secure protocol, Spontaneous Network, Adhoc network, Symmetric/asymmetric key, Encryption, Authentication.

I. INTRODUCTION

In the mobile communication have exponential growth due to the mobility, accessing information from anywhere, anytime, easy deployment, and user friendly. There is no proper security in this type of wireless communication. For an example we send a photo between the user have less security but the government information need the more authentication for the exchange of data. A spontaneous ad hoc network is type of ad hoc network that is formed in a certain time during a period of time, with no dependence on a central server and without the intervention of an expert user, in order to solve a problem or carry out a specific task . This network is built by several independent nodes coming together at the same time and in the same place to be able to communicate with each other. Nodes are free to enter and leave the network and they could be mobile or not. Spontaneous networking happens when neighbouring nodes discover each other within a short period of time; however, the velocity of discovery is paid in terms of energy consumption. Spontaneous networks are conceptually in a higher level of abstraction than ad hoc ones; they are basically those which seek to imitate human relationships in order to work together in groups, running on an existing technology. Their objective is the integration of services and devices in an environment which allows the provision to the user of an instant service with minimum manual intervention.

Spontaneous networks are created in a situation where devices are placed close to each other i.e. within a range of Wi-Fi. Consider an example, if you want to buy a medicine from the medical shop. You find shop is closed, in such situation; you will perform following steps:

Join Wi-Fi network of shop
Access services given by shop owner
Enter necessary information related to medicine
Select the needed medicine and enter your address and contacts
Send to your location which you chosen.
Leave network

To perform all these tasks you just connect to shop's network without internet connection and access the services, is called spontaneous network.

©IJRASET 2015: All Rights are Reserved

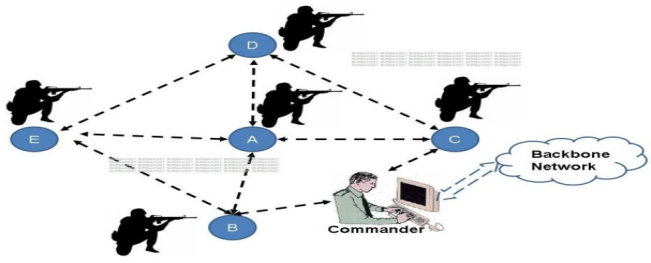
Just create network among wireless devices, placed close to each other for small period of time, join new user into the network, access services and resources and leave the network without any central infrastructure. First user creates the network and does all global settings like SSID, IP address space, session key generation etc. Just creating the network without security may be vulnerable to attacks so some security is required for managing network. I have develop a secure protocol for wireless spontaneous network which provides various security measures for network. They have implemented authentication mechanism at the time of joining new user into the network. For authentication they used public key cryptography for transmitting packets. After accessing necessary information retrieve the specific task and leave the network.

A. Spontaneous Network Proposal Description

If some people wish to build a spontaneous network, they may meet in a physical space at a given moment in order to make use of services such as group communication, cooperation on running programs, security, and so forth. The members who make up this community may vary at any specific time (users may join or leave at will).
When a device joins the network, it must follow the following steps.

1) Integration of the Device into the Network.
2) Agree the transmission protocol and speed.
3) Configure node addresses, routing information and other resources.
4) Discovery of the Services and Resources Offered by the Devices.
5) Discover the services and resources shared in the network.
6) Have a list of services and resources available in the network updated.
7) Access to the Services Offered by the Devices.
8) Manage the automatic integration tasks and the use of, for example, agent service.
9) Manage access security to the services.
10) Manage the join and the leave of nodes of the network.
11) Collaborative Tasks.
12) Within the intranet, among the various members.
13) On the internet, with the other communities.

This spontaneous network used for the authentication of in real time application like military services.



Military Ad-hoc Network

II. EXISTING SYSTEM

The objective of the existing system, the adhoc networks consist of a collection of wireless nodes, which communicate over common wireless medium. Adhoc network must operate independent of any infrastructure, while still providing administrative

©IJRASET 2015: All Rights are Reserved

services needed to support the functionalities, like address allocation, name resolution, service location, and an authentication. The limited nodes are involved in the network. The energy constraints are less in the transmission of the packets. So the packet has been dropped at the receiving end. The authentication is less compare to the spontaneous network.

In order to solve these issues it is necessary to leverage some aspect of the environment in which to create the spontaneous network.

A. Drawbacks in existing system

Frequency has been fixed in the previous network. All nodes may not be able to execute routing by use of security protocols. Energy, node variability, error rate, and bandwidth limitations are affect the network. Security mechanisms are not properly followed. Dynamic networks with flexible memberships, group signatures, and distributed signatures are difficult to manage.

In the reliable communication has node authorization, key exchange, security methods are main issue in mobile ad hoc network. For an authentication use the secret key, such as pre-distribution key algorithms, symmetric and asymmetric algorithms, intermediate node-based methods, and hybrid methods are used. But these methods are not enough for spontaneous networks because they need an initial configuration or external authorities.

III. RELATED WORK

Lot of proposal has been done in the spontaneous network. L.M.Feeney, proposed the concept of spontaneous network and the features. IP addressing is one of the important part while create the network. IP address configuration in spontaneous network has been explained by R.Lucesta. Prof. D.N.Rewadkar have given energy efficient protocol for spontaneous network. Spontaneous need the manual energy not actual battery of laptop is one of the major issue which is overcome in the proposal. R. Lacuesta, J. Lloret have explained the security attack and architecture of the spontaneous network.

Atul Kahate has provided the cryptography and network security. Study of literature survey some issues done during the communication via like Bluetooth compare to wifi. Node energy is not proper for the communication because of dropped packets at the receiving end. In our proposal system we are implement the spontaneous network which will use for the authentication and save the packets without drop.

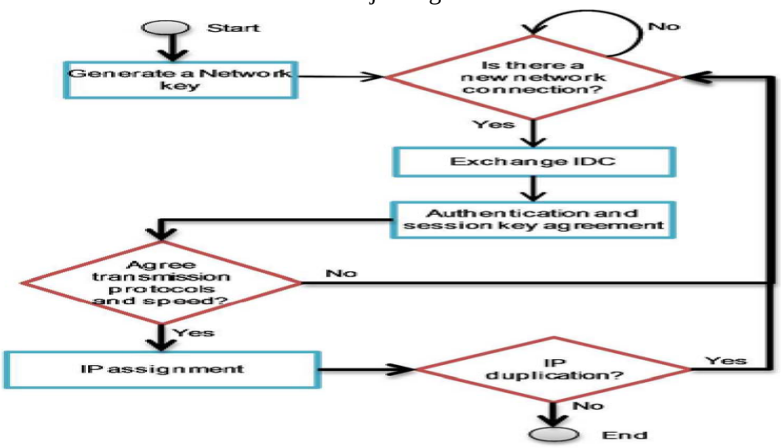
IV. SECURE NETWORK

A. Network Overview

The self-configure secure protocol allows the creation and management of distributed and decentralized spontaneous networks with little involvement from the user, and the combination of different devices (PDAs, cell phones, laptops, etc.). Collaboration between the devices allows condition and access to different services, such as group communication, relationship in program delivery, security, etc. The network members are free to join or leave the network after completion of the task. Spontaneous network should complete the following steps in order to be created.

The network will be secured by using this protocol functions.

Procedure for joining a new node



©IJRASET 2015: All Rights are Reserved

B. Joining Nodes in the Network

The first node creates the network and generates a random session key, which will be exchanged with new nodes after the authentication phase. The phases of a node joining the network: node authentication and authorization, agreement on session key, transmission protocol and speed, and IP address and routing.

When node B wants to join an existing network, it must choose a node within communication range to authenticate with (e.g., node A). A will send its public key. Then, B will send its Identity Card signed by A's public key. Next, A validates the received data and verifies the hash of the message in order to check that the data has not been modified. In this step, A establishes the trust level of B by looking physically at B (they are physically close), depending on whether A knows B or not. Finally, A will send its Identity Card data to B (it may do so even if it decides not to trust B).

This data will be signed by B's public key (which has been received on B's Identity Card). B will validate A's Identity Card and will establish the trust and validity in A only by integrity verification and authentication. If A does not reply to the joining request, B

must select another network node (if one exists). After the authentication, B can access data, services, and other nodes certificates by a route involving other nodes in network.

C. Providing Services

B asks for the available services. Services can be discovered using web services description language (WSDL). A user can ask other devices in order to know the available services. It has an agreement to allow access to its services and to access the services offered by other nodes. Services have a large number of parameters which are not transparent to the user and require manual configuration. One issue is to manage the automatic integration tasks and use, for example, service agents. Other is to manage secure access to the services offered by the nodes in the network.

The fault tolerance of the network is based on the routing protocol used to send information between users. Services provided by B are available only if there is a path to B, and disappear when B leaves the network.

D. Establishing trusted chain between the trust users

There are only two trust levels in the system. Node A either trusts or does not trust another node B. The software application installed in the device asks B to trust A when it receives the validated IDC from B. Trust relationship can be asymmetric. If node A did not establish trust level with node B directly, it can be established through trusted chains, e.g., if A trusts C and C trusts B, then A may trust B. Trust level can change over time depending on the node's behaviour. Thus, node A may decide not to trust node B although A still trusts C and C trusts B anymore. It can also stop trusting if it discovers that chain not exist anymore.

V. PROTOCOL AND NETWORK MANAGEMENT

In the network formation, nodes perform an initial exchange of configuration information and security using the mechanism of authentication. This mechanism avoids the need for a central server, making the tasks of building the network and adding new members very easy. The network is created using the information provided by users, thus, each node is identified by an IP address. Services are shared using TCP connections. The network is built using IEEE 802.11b/g technology which has high data rates to share resources. We have reserved the short-range technology (Bluetooth) to allow authentication of nodes when they join the network. After the authentication process, each node learns the identity card of other known nodes, a public key and a LID. This information will be updated and completed throughout the network nodes. This structure provides an authenticated service that verifies the integrity of the data from each node because there is a distributed CA. Each node requests the services from all the nodes that it trusts, or from all known nodes in the network, depending on the type of service. A request to multiple nodes is made through diffusion processes. The protocol prioritizes access to information through trusted nodes.

When the information cannot be obtained through these nodes, it can then ask other nodes.

A. Network creation

The first node in the network will be responsible for setting the global settings of the spontaneous network. However, each node must configure its own data (including the first node): IP, port, data security, and user data. This information will allow the node

©IJRASET 2015: All Rights are Reserved

to become part of the network. After this data are set in the first node, it changes to standby mode.

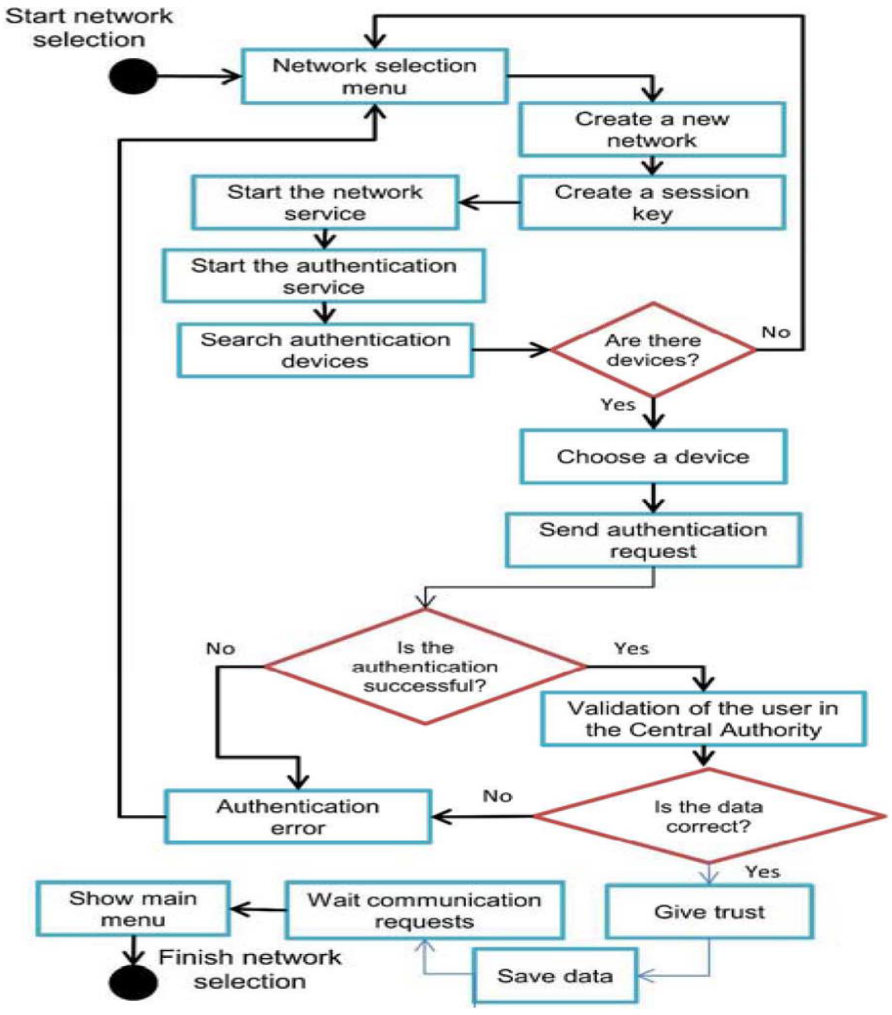
B. Joining the new members

The second node first configures its user data and network security. Then, the greeting process starts. It authenticates against the first node. The connection is created through a short-range link technology, to provide flexibility and ease of detection and selection of nodes, and visual contact with the user of the node. Furthermore, minimal involvement of the user is required to configure the device, mainly to establish trust. This technology also limits the scope and the consumption of involved nodes. Each additional node authenticates with any node in the network.

C. Protocol Functionalities

Once the validation/registration process of the user in the device has been done, he/she must determine whether to create a new network or participate in an existing one. If he/she decides to create a new network. First, a session key will be generated. Then, the node will start its services (including the network and authentication services).

New network creation procedure



Finally, it will wait for requests from other devices that want to join the network. If the user wants to become part of an existing network to find a device that will give trust to it, save corresponding data and will able to begin communications.

©IJRASET 2015: All Rights are Reserved

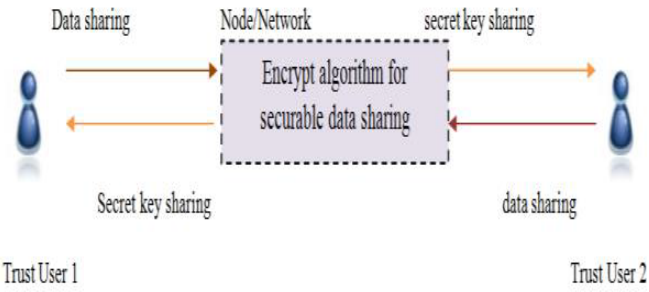
When the node is authenticated, it is able to perform several tasks. Some of them are performed transparently for the user, but others are used by the user to perform some
operations in the network. They are the user application options.
The authenticated node can perform the following tasks:

1) Display the nodes.
2) Modify the trust of the nodes.
3) Update the information.
4) Other nodes certificate request.
5) Process an authentication request
6) Forward an information request
7) Send data to one node/ all node
8) Modify the data
9) Leave the network

D. Data transfer between the node

A node receives a data packet that is encrypted with AES algorithm. When the server process received the packet, it is decrypted at the user side.

VI. SYSTEM ARCHITECHTURE



A. Architecture diagram for Secure Protocol for Spontaneous Wireless Ad Hoc Networks Creation

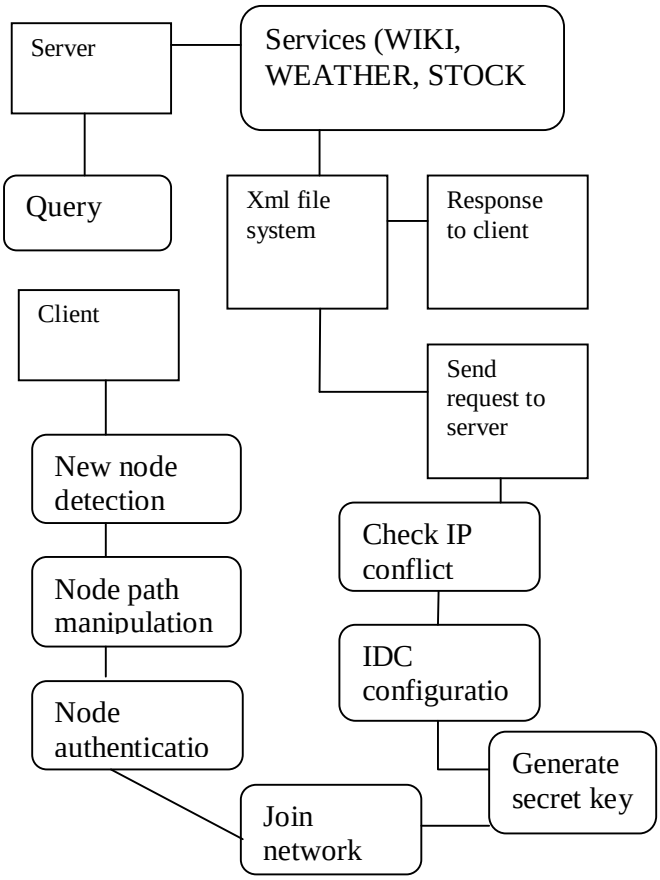
This diagram shows secret key and data sharing between a two trusted user. If a new node want to with the existing node, the new node will send the request to the existing node. Based on the request, the existing node will send its public key to the new node. After that the new node and existing node will share their public and private key components to authenticate each other. For security purpose the data will be encrypted during transmission. This step enables devices to communicate, including the automatic configuration of logical and physical parameters. The system is based on the use of an IDentity Card (IDC) and a certificate.

The IDC contains public and private components. The public component contains a Logical Identity (LID), which is unique for each user and allows nodes to identify it. It may include information such as name, photograph or other type of user identification. This idea has been used in other systems such as in vehicular ad hoc networks . It also contains the user's public key , the creation and expiration dates, an IP proposed by the user, and the user signature. The user signature is generated using the Secure Hash Algorithm (SHA-1) on the previous data to obtain the data summary. Then, the data summary is signed with the user's private key. The private component contains the private key. The user introduces its personal data (LID) the first time he/she uses the system because the security information is generated then. Security data are stored persistently in the device for future use.

©IJRASET 2015: All Rights are Reserved

Volume 3 Issue IV, April 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

B. System Design Process



Validation of integrity and authentication is done automatically in each node. The certification authority for a node could be any of the trusted nodes. This system enables us to build a distributed certification authority between trusted nodes. When node A wants to communicate with another node B and it does not have the certificate for B, it requests it from its trusted nodes. After obtaining this certificate the system will validate the data; if correct then it will sign this node as a valid node. All nodes can be both clients and servers, can request or serve requests for information or authentication from other nodes.

VII. PROPOSED SYSTEM

The network and protocol proposed in this paper can establish a secure self-configured environment for data distribution and resources and services sharing among users. Security is established based on the service required by the users, by building a trust network to obtain a distributed certification authority. A user is able to join the network because he/she knows someone that belongs to it. Thus, the certification authority is distributed between the users that trust the new user. The network management is also distributed, which allows the network to have a distributed name service. We apply asymmetric cryptography, where each device has a public-private key pair for device identification and symmetric cryptography to exchange session keys between nodes. There are no anonymous users, because confidentiality and validity are based on user identification.

A. Advantages of proposed system

We presented the basis to setup a secure spontaneous network. To solve mentioned security issues, we used an authentication

©IJRASET 2015: All Rights are Reserved

phase and a trust phase. We presented a mechanism to allow nodes to check the authenticity of their IP addresses while not generating duplicated IP addresses. The mechanism helps nodes to authenticate by using their IP addresses. We have used this mechanism in the secure protocol presented in this paper, but it can be replaced by any other IP address assignment mechanism.
It presents two secure and energy-saving spontaneous ad hoc protocols for wireless mesh client networks where two different security levels (weak and strong) are taken into account in the path when information is transmitted between users. These public keys are used to calculate a shared secret session key for encrypted communication. a secure spontaneous network protocol based on user trust that provides node authenticity, integrity checking, and privacy.

VIII. CONCLUSION

The creation of a spontaneous wireless adhoc network is described here in this paper. It is based on a social network imitating the behaviour of human relationships. Thus, each user will work to maintain the network, improve the services offered, and provide information to other network users. The protocol provided some procedures for self-configuration: a unique IP address is assigned to each device, the DNS can be managed efficiently and the services can be discovered automatically.
It also created a user-friendly application that has minimal interaction with the user. The response times obtained are suitable for use in real environments, even when devices have limited resources. Storage and volatile memory needs are quite low and the protocol can be used in regular resource-constrained devices (cell phones, PDAs...).
The propose system to add some new features to the user application (such as sharing other types of resources, etc.) and to the protocol, such as an intrusion detection mechanism and a distributed Domain Name Service by using the LID and IP of the nodes. Now, we are working on adding other types of nodes that are able to share their services in the spontaneous network.

IX. FUTURE ENHANCEMENT

We propose to add some new features to the user application (such as sharing other types of resources, etc.) and to the protocol, such as an encryption decryption mechanism and a distributed Domain Name Service by using the LID and IP of the nodes. Now, we are working on adding other types of nodes that are able to share their services in the spontaneous network without loss of data packets. The designing of complete self configured secure protocol that is able to create network and share secure services without any external infrastructure. Using cryptographic secret key technique to improve a level of security. Users easily join the network access the information and leave the network after completion of task without any loss of data and external sources.

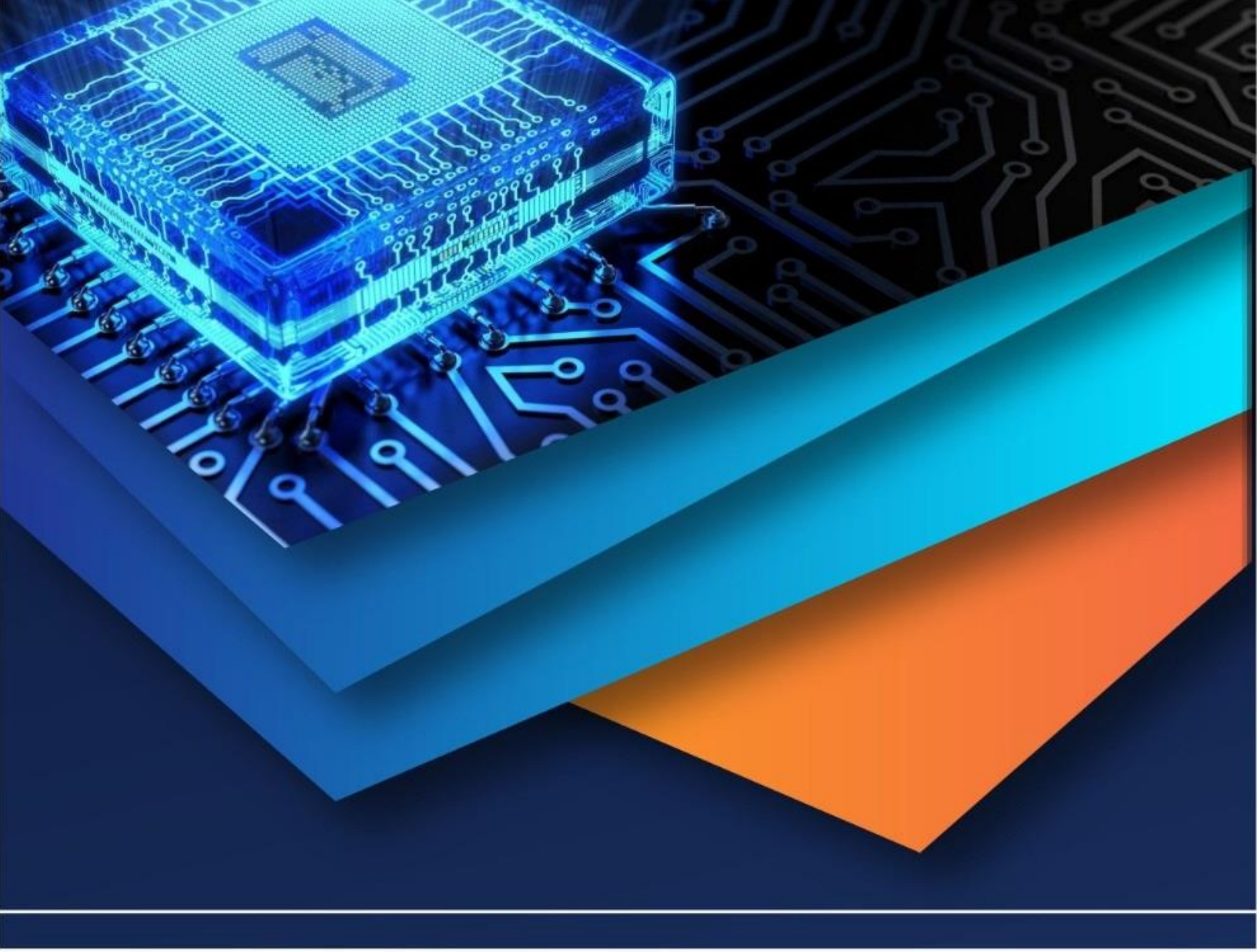
REFERENCES

[1] L.M. Feeney, B. Ahlgren, and A. Westerlund, “Spontaneous Networking: An Application-Oriented Approach to Adhoc Networking,” IEEE Comm. Magazine, vol. 39, no. 6, pp. 176-181, June 2001.
[2] J. Lloret, L. Shu, R. Lacuesta, and M. Chen, “User-Oriented and Service-Oriented Spontaneous Ad Hoc and Sensor Wireless Networks,” Ad Hoc and Sensor Wireless Networks, vol. 14, nos. 1/ 2, pp. 1-8, 2012.
[3] S. Preuß and C.H. Cap, “Overview of Spontaneous Networking - Evolving Concepts and Technologies,” Rostocker Informatik- Berichte, vol. 24, pp. 113-123, 2000.
[4] R. Lacuesta, J. Lloret, M. Garcia, and L. Pen˜ alver, “A Spontaneous Ad-Hoc Network to Share WWW Access,” EURASIP J. Wireless Comm. and Networking, vol. 2010, article 18, 2010.
[5] Y. Xiao, V.K. Rayi, B. Sun, X. Du, F. Hu, and M. Galloway, “A Survey of Key Management Schemes in Wireless Sensor Networks,” Computer Comm., vol. 30, nos. 11/12, pp. 2314-2341, Sept. 2007.
[6] V. Kumar and M.L. Das, “Securing Wireless Sensor Networks with Public Key Techniques,” Ad Hoc and Sensor Wireless Networks, vol. 5, nos. 3/4, pp. 189-201, 2008.
[7] S. Zhu, S. Xu, S. Setia, and S. Jajodia, “LHAP: A Lightweight Hopby- Hop Authentication Protocol For Ad-Hoc Networks,” Ad Hoc Networks J., vol. 4, no. 5, pp. 567-585, Sept. 2006.
[8] A. Noack and S. Spitz, “Dynamic Threshold Cryptosystem without Group Manager,” Network Protocols and Algorithms, vol. 1, no. 1, Oct. 2009.
[9] J. Yan, J. Ma, F. Li, and S.J. Moon, “Key Pre-distribution Scheme with Node Revocation for Wireless Sensor Networks,” Ad Hoc and Sensor Wireless Networks, vol. 10, nos. 2/3, pp. 235-251, 2010.
[10] M. Mukesh and K.R. Rishi, “Security Aspects in Mobile Ad Hoc Network (MANETs): Technical Review,” Int’l J. Computer Applications, vol. 12, no. 2, pp. 37-43, Dec. 2010.
[11] K. Sahadevaiah and P.V.G.D. Prasad Reddy, “Impact of Security Attacks on a New Security Protocol for Mobile Ad Hoc Networks,” Network Protocols

©IJRASET 2015: All Rights are Reserved

and Algorithms, vol 3, no. 4, pp. 122-140, 2011.
[12] L. Herrero and R. Lacuesta, "A Security Architecture Proposal for Spontaneous Networks," Proc. Int'l Conf. Advances in the InternetProcessing System and Interdisciplinary Research, Oct. 2003.
[13] R. Lacuesta and L. Pen˜ aver, "IP Addresses Configuration in Spontaneous Networks," Proc. Ninth WSEAS Int'l Conf. Computers (ICCOMP '05), July 2005.
[14] R. Lacuesta and L. Pen˜ alver, "Automatic Configuration of Ad-Hoc Networks: Establishing Unique IP Link-Local Addresses," Proc. Int'l Conf. Emerging Security Information, Systems and Technologies (SECURWARE '07), 2007.
[15] J. Latvakoski, D. Pakkala, and P. Paakkonen, "A Communication Architecture for Spontaneous Systems," IEEE Wireless Comm., vol. 11, no. 3, pp. 36-42, June 2004.
[16] L. Liu, J. Xu, N. Antonopoulos, J. Li, and K. Wu, "Adaptive Service Discovery on Service-Oriented and Spontaneous Sensor Systems," Ad Hoc and Sensor Wireless Networks, vol. 14, nos. 1/2, pp. 107-132, 2012.
[17] S. Gallo, L. Galluccio, G. Morabito, and S. Palazzo, "Rapid and Energy Efficient Neighbor Discovery for Spontaneous Networks," Proc. Seventh ACM Int'l Symp. Modeling, Analysis and Simulation of Wireless and Mobile Systems, Oct. 2004.
[18] J. Ba¨ckstro¨m and S. Nadjm-Tehrani, "Design of a Contact Service in a Jini-Based Spontaneous Network," Proc. Int'l Conf. and Exhibits on the Convergence of IT and Comm., Aug. 2001.
[19] V. Untz, M. Heusse, F. Rousseau, and A. Duda, "Lilith: an Interconnection Architecture Based on Label Switching for
Spontaneous Edge Networks," Proc. First Ann. Int'l Conf. Mobile and Ubiquitous Systems: Networking and Services (Mobiquitous '04), Aug. 2004.
[20] L.M. Feeney, B. Ahlgren, A. Westerlund, and A. Dunkels, "Spontnet: Experiences in Configuring and Securing Small
Ad Hoc Networks," Proc. Fifth Int'l Workshop Network Appliances, Oct. 2002.
[21] M. Danzeisen, T. Braun, S. Winiker, D. Rodellar, "Implementation of a Cellular Framework for Spontaneous Network Establishment," Proc. IEEE Wireless Comm. and Networking Conf. (WCNC '05), Mar. 2005.
[22] J. Rekimoto, "SyncTap: Synchronous User Operation for Spontaneous Network Connection," Personal and Ubiquitous Computing, vol. 8, no. 2, pp. 126-134, May 2004.
[23] C. Cornelius, A. Kapadia, D. Kotz, D. Peebles, M. Shin, and N. Triandopoulos, "Anonysense: Privacy-Aware People-Centric Sensing," Proc. Sixth Int'l Conf. Mobile Systems, Applications, and Services (MobiSys '08), pp. 17-20, June 2008.
[24] R. Lacuesta, J. Lloret, M. Garcia, and L. Pen˜ alver, "Two Secure and Energy-Saving Spontaneous Ad-Hoc Protocol for Wireless Mesh Client Networks," J. Network and Computer Applications, vol. 34, no. 2, pp. 492-505, Mar. 2011.
[25] J. Sun, C. Zhang, Y. Zhang, and Y. (Michael) Fang, "An Identity- Based Security System for User Privacy in Vehicular Ad Hoc Networks," IEEE Trans. Parallel and Distributed Systems, vol. 21, no. 9, pp. 1227-1239, Sept. 2010.

©IJRASET 2015: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)