International Journal of Electrical and Electronics Research ISSN 2348-6988 (online)
Vol. 3, Issue 1, pp: (242-248), Month: January - March 2015, Available at: www.researchpublish.com

Enhance Security for Spontaneous Wireless Ad Hoc Network Creation

[1]Kiran Shinde, [2]Prof. Harjeet Kaur,[3]Prof. Sharad Wagh

[1,2]University of Pune, [3]University of Mumbai
[1,2]Indira College of Engg. And Mngm. Pune, India
[3]MPSTME, Mumbai, India

***Abstract*: In An mobile ad hoc network must operate independent of pre established or centralized network management Infrastructure, while still providing administrative services needed to support applications. Address allocation, name resolution, service location, authentication, and access control policies represent just some of the functionality that must be supported - without pre configuration or centralized services in this paper spontaneous wireless ad hoc network creation no need of any infrastructure no need of any administrator for handling the services. No need of any external support for handling functionalities of network. All the services are provided without fixed infrastructure whoever is present in the network. This protocol allows sharing of resources and services among users in secure environment. In human communication model, two people those are physically closed to each other can talk directly without any server. In spontaneous network there is no server or any infrastructure between nodes to communicate, anybody those who wants to communicate can join, communicate and leave the network without any central server. It is based on peer to peer network. In this paper, we study all work to be done on spontaneous network and various security mechanisms to be provided.**

***Keywords:* Spontaneous networks, wireless network, secure protocol, IDC, MANET.**

I. INTRODUCTION

In last few years mobile ad-hoc network (MANET) is quickly developed and widely used. Mobile ad-hoc network is created without infrastructure with a collection of mobile nodes. Manet is a group of wireless nodes without support of external infrastructure. To achieve a reliable connectivity and node authentication in MANET key exchange mechanism is required for authentication. Security methods are required such as symmetric and asymmetric algorithm, hybrid methods, pre distribution key algorithm, intermediate node based methods. Spontaneous network is a solution of these problems of MANET. Spontaneous network is special case of mobile ad-hoc network. It is work like a human interaction. In human communication model, people come together form a group and start talking or communicating with each other by sharing their views, information and many things. During this eye to eye communication anybody can talk, join the group or leave the group without getting any permission. There is not any central organizer. But the problem is, if someone leaks any confidential information to other person therefore security is very important. Spontaneous network is work like human communication where wireless nodes are placed together for communication to share resources and services for limited period and limited space. Spontaneous network is wired or wireless but for this paper we will consider only wireless network. In this network new services can be added without intervention of users in the network. Failure or breakdown of any service or any nodes will not compromise the functionality of network.

Features of spontaneous network are defined below.

1) Network boundaries are poorly defined: - in convention network simply means enabling the network interface and connecting to networking infrastructure. This network expected to put node into contact with all necessary services.

2) The network is not planned: - design of conventional network is a part of system administrator logical and administrative boundaries will define where the services will be applied and where it replicated. In conventional network firewalls are used for security. But in ad-hoc network node must create network infrastructure in cooperation with untrusted partner where boundaries are not defined like where it accepts inside and filter outside the network.

3) Hosts are not pre configured: - in spontaneous networks network must be created anywhere and anytime with any participants. This can be limit the amount of administrative and configuration information must be preconfigured on node. Information such as host name, addresses of node, and available services and nodes where hosted cannot be predetermined hence hosts and nodes are not preconfigured in the network.

4) There are no central servers: - servers are very problematic for networks because nodes from servers have to agree either promote the backup or reinitialize the services. If the two nodes are from two different servers then they have to synchronize. This is not happened in the spontaneous network where user can disconnect any time from home network can rejoin any time in spontaneous network. Consider a user who wishes to send mail to Colleague who is a part of same spontaneous Network he may attempt to send it via spontaneous network before queuing it to send via infrastructure network.

II. REVIEW

Related literature survey shows so many security methods such as re distribution key algorithm symmetric and asymmetric algorithm but this methods are not suitable for spontaneous networks because they need configuration of

Network and external authorities. Secure spontaneous network protocol is based on the user trust which provides node authenticity, integrity checking, confidentiality. For node authentication and trust wireless network uses certificate authority.

III. SECURE SPONTANEOUS NETWORK

This protocol allows creating and managing distributed and decentralized spontaneous network. Cooperation of different devices can allows to access different services like group communication, security etc. members and services can be changed because the network allows devices to join and leave the network any time. 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. Spontaneous network should complete the following steps in order to be created [1].

A. Node joining:

Joining procedure is depending on IDC i.e. identity card which is holds by every user which is in network or not. IDC contains public as well as private key information public components contain logically identity which is unique for every user which uses for identification of node it also contains information such as name photographs or other user identification documents. It also contains public key, creation and expiration dates, an ip proposed by the user and user signature which is created by secure hash algorithm (SHA- 1) [2]. Private components contains private key. Which is in communication range to validate itself (e.g. Node A) A will send its public key. Then, B will send its IDC 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 IDC 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 IDC) [3]. B will validate A's IDC 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 services, data and other nodes certificates by a route involving other nodes in network. Once the A node is validated then session key which is randomly created by first node of network is then distributed to all nodes of network. For the node joining combination of symmetric and asymmetric key is used symmetric key is used for session key to encrypt the confidential message for that advanced encryption standard (AES) algorithm is used. Because AES requires less time for execution and low energy consumption. Whereas asymmetric key cryptography is used for user identification and session key distribution which uses Rivest, Shamir and Adelman cryptography algorithm (RSA) is use for asymmetric key cryptography .finally the ip for new node is created and checked for ip duplication. The first node in the network will be

responsible for setting the global settings of the spontaneous network (SSID, session key). However, each node must configure its own data (including the first node): IP, data, port, and user data. This information will help the node to become part of the network.

B. Service discovery:

B asks for the services. Services can be discovered by web services description language (WSDL). Our model is based on [4]. But in our spontaneous network we don't use a central server. Moreover, other service discovery Services can be implemented in our system [5].User can ask to other devices for available services it has an agreement to use available services and the services offered by other nodes. Services provided by B are available only if there is a path to B, and disappear when B leaves the networked.

C. *Trust chain*:

There are only two trust levels in the system, either trust or does not trust. Node A either trusts or does not trust another node B. The user interface of application installed in the device asks B to trust A when it receives the validated IDC from A. Trust Relationship can be asymmetric. If node A did not establish trust level with node B directly, it can be established through trusted Chains network, e.g., if A node trusts C node and C node trusts B node, then A node may trust B node. Trust level can change over time depending on the node's behavior. Thus, node A may decide not to trust node B although A still trusts C and C trusts B. It can also stop trusting if it discovers that previous trust chain does not exist anymore [6], [7].

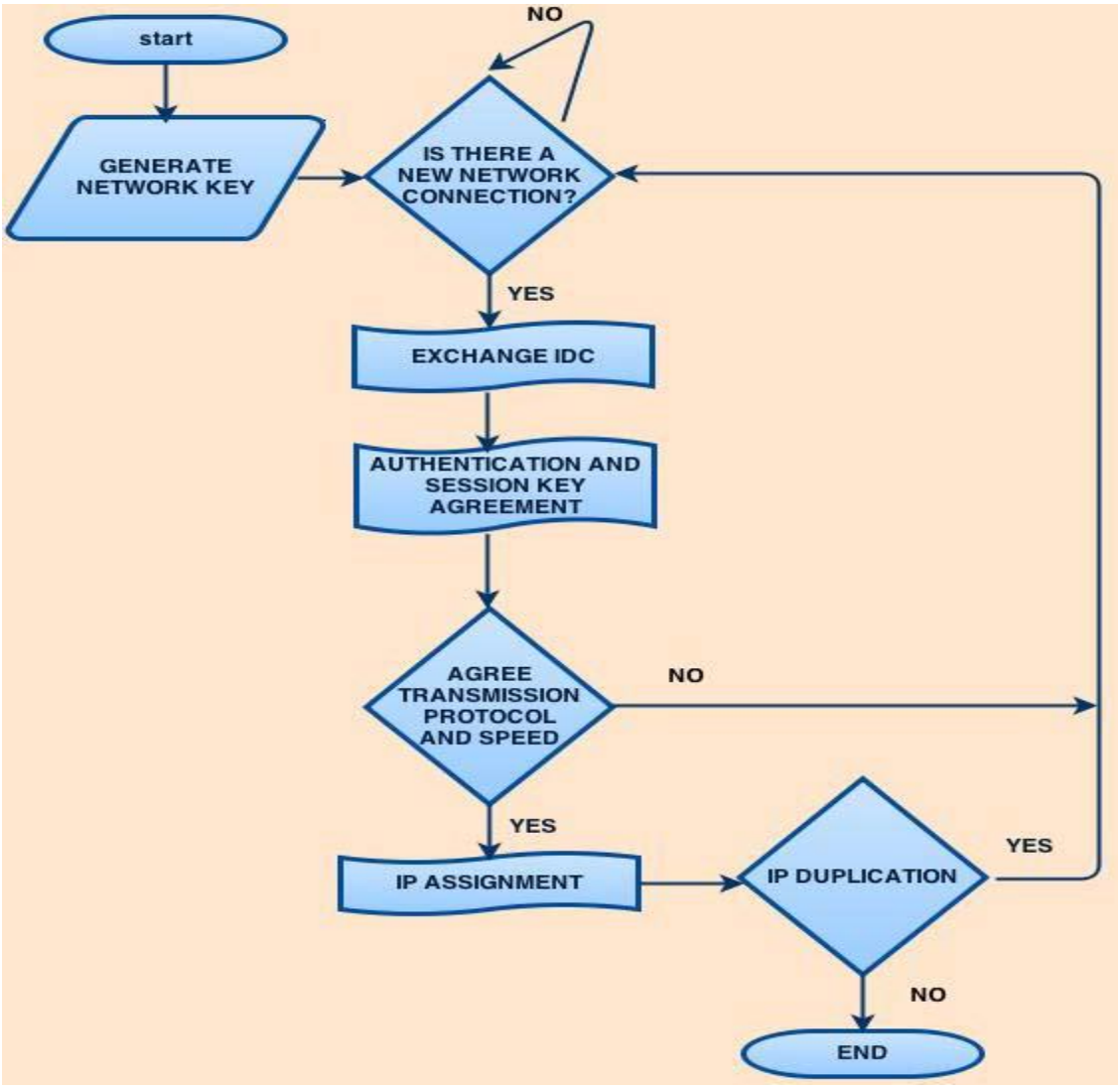


Fig.1. Node joining

IV. SIMULATION SCENARIO

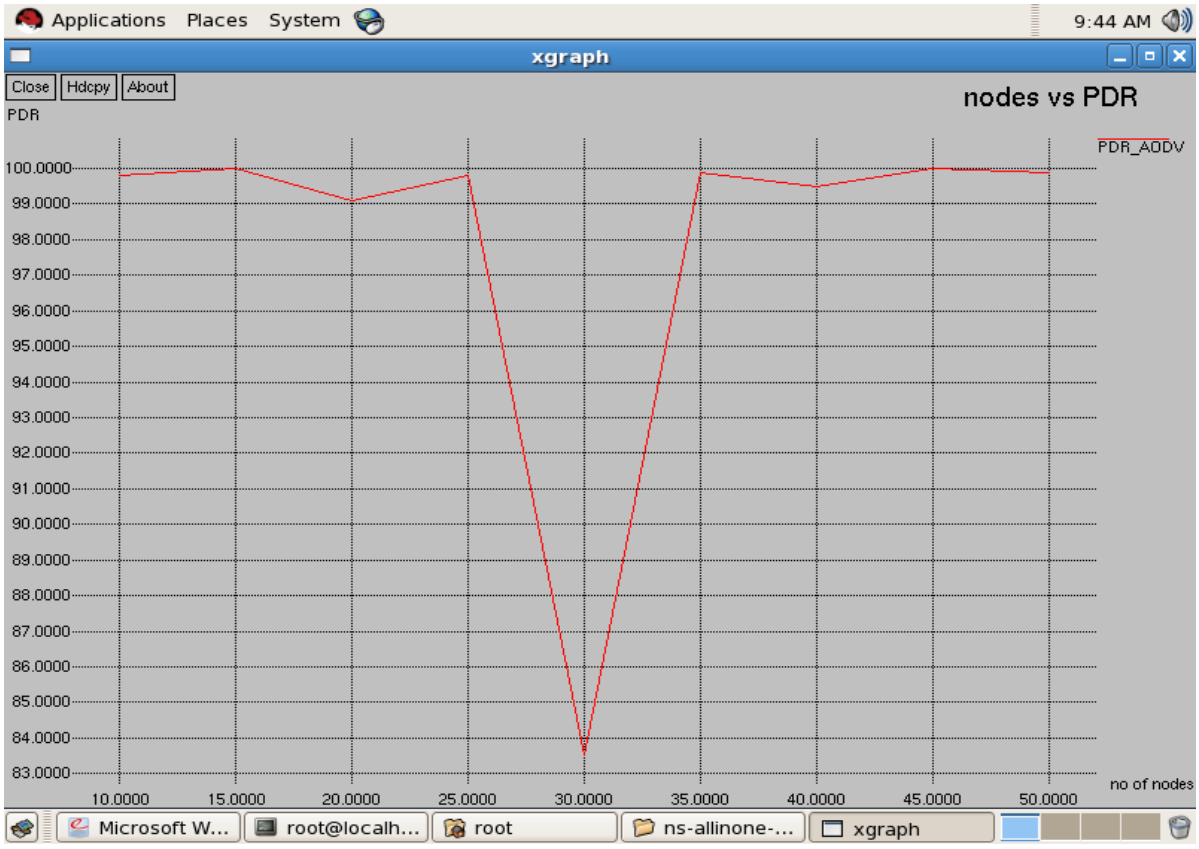
In this section, wireless network performance depends mainly on the end to end. We are going to present simulation scenario aimed at activating the network security through network throughput, packet transfer between nodes within the scenario. Simulation principles and strategies fulfill the achievement of simulation for specific protocols and the configuration nodes and establishment of network simulation environment respectively. Table 1 refers parameter using in scenario, using the aided software like NAM to make a further study, and simulation process and results analysis. First of all, we set the topology and the configuration of nodes properties and also properties of MAC layer like address type, protocol type, channel type, simulation time, modulation type, tx, rx, idle, sleep power and transmission way of wireless. The following is the parameters of simulation scenario figure 7 and nodes layout before transferring information between them.

TABLE I. SINULATION PARAMETERS

Parameters	**Values**
Area of simulation	(500*500)m
Nodes no.	Variable
Types of routing protocol	AODV
Internet protocol type	Tcp
Antenna model	Omni directional
Type of the Mac	802.11
Transmission speed	30m/s
Area of simulation	(500*500)m
Nodes no.	Variable

TABLE: II. SINULATION RESULTS

Nodes	**Packet delivery ratio**	**Throughput**	**Avg energy consumption**
10	100	95410.2	1.4827
15	99.7953	95132.2	1.54997
20	100	95410.2	0.267309
25	100	95410.2	0.580127
30	100	95410.2	0.180496
35	100	95410.2	0.156115
40	100	95410.2	0.134846
45	100	95410.2	0.12193
50	99.8976	95237.1	1.575
55	100	95410.2	0.100833
60	79.1198	90970	1.36401



Fig,2. Graph of nodes vs pdr

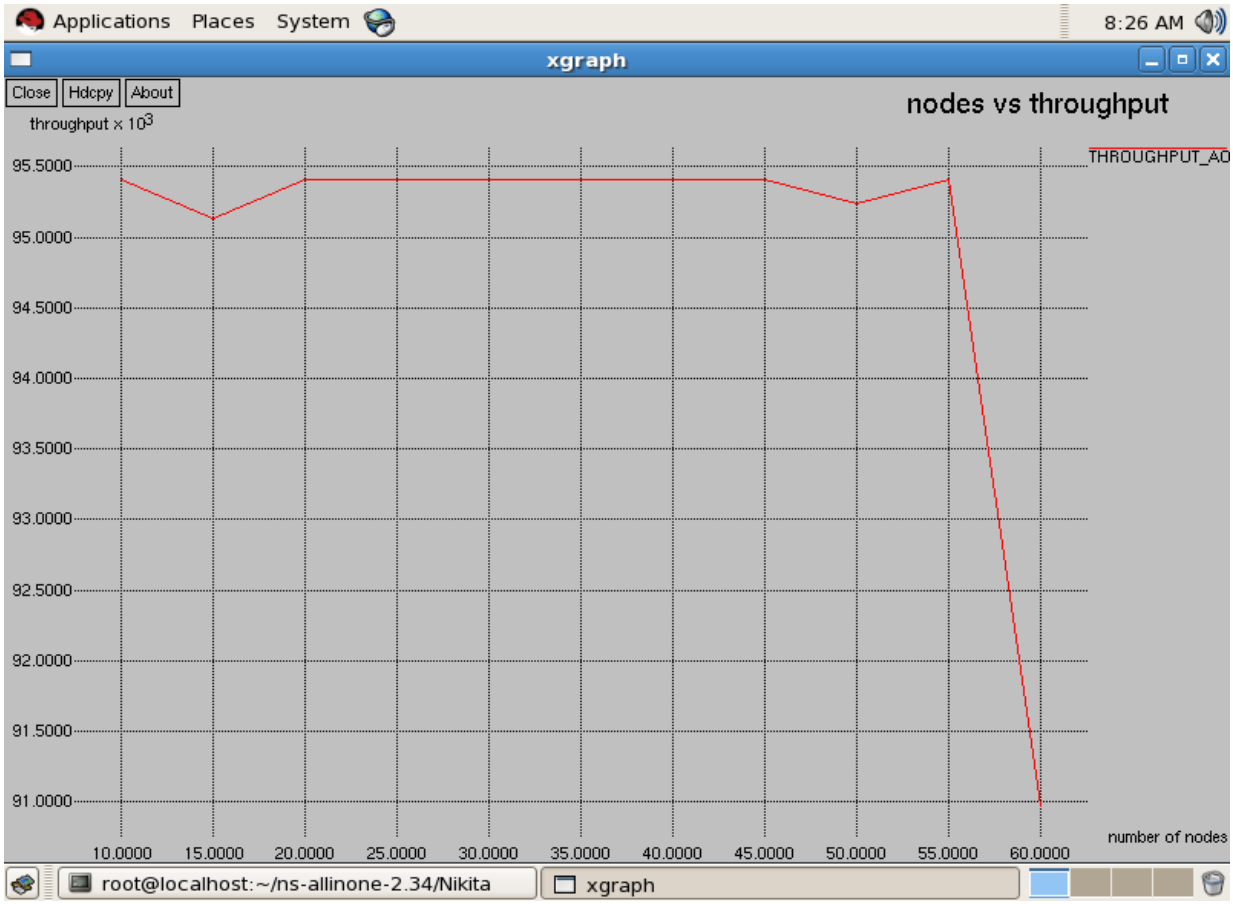


Fig.3. Graph of nodes vs. throughput

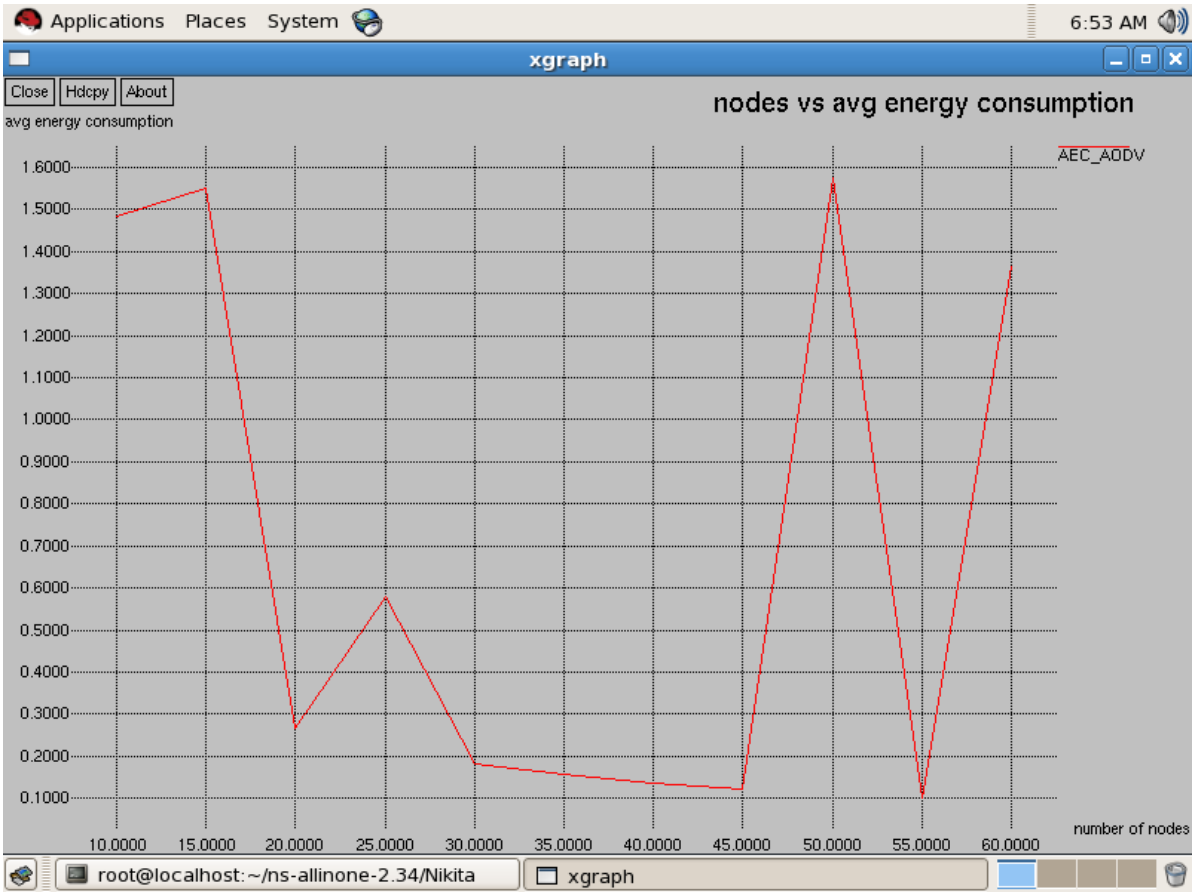


Fig.4. Graph of nodes vs. energy consumptions

V. CONCLUSION

In this paper, the software tool Network Simulator (Version 2), widely known as ns-2, is described and used for the simulation of selected illustrative examples of wireless networks. In general, ns2 provides users with a way of specifying network protocols and simulating their behavior. The result of the simulation are transfer information secure between nodes .In the paper we have ns2.34 simulator the end user performance of wireless network consisting variable nodes ,the simulation result in following conclusion about network behavior: First is transfer information package between nodes. For future work to use cryptography algorithm as (hybrid) to more secure information transfer among nodes.

REFERENCES

[1] L.M. Feeney, B. Ahlgren, and A. Wasterlund, "Spontaneous Networking: An Application-Oriented Approach to Ad-hoc Networking," IEEE Comm. Magazine, vol. 39, no. 6, pp. 176-181, June 2001.

[2] FIPS 180-1 - Secure Hash Standard, SHA-1, "National Institute of Standards and Technology,"http:// www. itl. nist.gov/ fipspubs/fip180-1.htm, Feb. 27, 2012.

[3] S. Zhu, S. Xu, S. Setia, and S. Jajodia, "LHAP: A Lightweight Hop by- Hop Authentication Protocol For Ad-Hoc Networks," Ad Hoc Networks J., vol. 4, no. 5, pp. 567-585, Sept. 2006.

[4] S.E. Czerwinski, B.Y. Zhao, T.D. Hodes, A.D. Joseph, and R.H. Katz, "An Architecture for a Secure Service Discovery Service," Proc. ACM/IEEE MobiCom '99, Aug. 1999.

[5] 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.

[6] Raquel Lacuesta, Jaime Lloret, Senior Member, IEEE, Miguel Garcia, Student Member, IEEE, and Lourdes Pen˜ alver-" A Secure Protocol for Spontaneous Wireless Ad Hoc Networks Creation",ieee transactions on parallel and distributed systems, vol. 24, no. 4, april 2013.

[7] 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.

[8] FIPS 180-1 - Secure Hash Standard, SHA-1, "National Institute of Standards and Technology," http://www.itl.nist. gov/fipspubs/ fip180-1.htm, Feb. 27, 2012.

[9] .A. Wander, N. Gura, H. Eberle, V. Gupta, and S. Chang, "Energy Analysis for Public-Key Cryptography for Wireless Sensor Networks," Proc. IEEE Third Int'l Conf. Pervasive Computing and Comm. (PerCom '05), pp. 8-12, Mar. 2005.

[10] N.R. Potlapally, S. Ravi, A. Raghunathan, and N.K. Jha, "Analyzing the Energy Consumption of Security Protocols," Proc. Int'l Symp. Low Power Electronics and Design (ISLPED '03), 2003.

[11] J. Goodman and A. Chandrakasan, "An Energy Efficient Reconfigurable Public-Key Cryptography Processor Architecture," Proc. Int'l Workshop Cryptographic Hardware and Embedded Systems (CHES '00), pp. 175-190, 2000.

[12] S. Landau, "Communications Security for the Twenty-First Century: The Advanced Encryption Standard," Notices of the Am. Math. Soc., vol. 47, no. 4, pp 450-459, Apr. 2000.

[13] J. Lo´pez and R. Dahab, "Performance of Elliptic Curve Cryptosystems," Technical Report IC-00-08, May 2000.

[14] R. Mayrhofer, F. Ortner, A. Ferscha, and M. Hechinger, "Securing Passive Objects in Mobile Ad-Hoc Peer-to-Peer Networks," Electronic Notes in Theoretical Computer Science, vol. 85, no. 3, pp. 105-121, Aug. 2003.

[15] S.E. Czerwinski, B.Y. Zhao, T.D. Hodes, A.D. Joseph, and R.H. Katz, "An Architecture for a Secure Service Discovery Service," Proc. ACM/IEEE MobiCom '99, Aug. 1999.

[16] L. Liu, J. Xu, N. Antonopoulos, J. Li, and K. Wu, "Adaptive Service Discovery on Service-Oriented and Spontaneous Sensor Systems," Adhoc and Sensor Wireless Networks, vol. 14, nos. 1/2, pp. 107-132, 2012.

[17] S. Capkun, L. Buttyan, and J.-P. Hubaux, "Self-Organized Public- Key Management for Mobile Ad Hoc Networks," IEEE Trans. Mobile Computing, vol. 2, no. 1, pp. 52-64, Jan.-Mar. 2003.

[18] T. Czachorski and F. Pekergin, "Diffusion Approximation as a Modeling Tool in Congestion Control and Performance Evaluation," Proc. Second Int'l Working Conf. Performance Modelling and Evaluation of Heterogeneous Networks (HET-NETs '04), July 26-28, 2004.

[19] R. Lacuesta and L. Herrero, "A Good Use of Bluetooth, A Good Use of Bluetooth," Proc. Int'l Workshop Advanced Web Eng. for e-Business (AWEEB '04), Mar. 21, 2004.

[20] The Legion of the Bouncy Castle Website, at h ttp://www.bouncycastle.org, Feb. 2012.

[21] Netbeans website, at: http://netbeans.org/, Feb. 2012.

[22] V.H. Zarate Silva, E.I. De la Cruz Salgado, and F. Ramos Quintana, "AWISPA: An Awareness Framework for Collaborative Spontaneous Networks," Proc. ASEE/IEEE 36th Frontiers in Education Conf., Oct. 2006.