# A Novel Secure Protocol for Spontaneous Wireless Ad Hoc Networks Creation

**Botcha Sandhya Rani [#1], Sri.M.Sampath Kumar [*2]**

[#1]M.Tech Scholar, [*2] Associate Professor
Department of Computer Science & Technology,
Andhra University College of Engineering,
Visakhapatnam, AP, (INDIA).

## Abstract

Now a day's wireless ad hoc networks are becoming more and more promising network in real time environment. These ad hoc networks using both symmetric and asymmetric schemes for performing network creations. In this paper we presented a new secure protocol for spontaneous wireless ad hoc networks which uses a hybrid symmetric/ asymmetric scheme and the trust between users in order to exchange the initial data and to exchange the secret keys that will be used to encrypt the data. Through this paper we want to convince that our proposal is a complete self-configured secure protocol that is able to create the network and share secure services without any predefined infrastructure. The protocol includes all functions needed to operate without any external support. We have designed and developed it in devices with limited resources. Network creation stages are detailed and the communication, protocol messages, and network management are explained. Our proposal has been implemented in order to test the protocol procedure and performance. Finally, we compare the protocol with other spontaneous ad hoc network protocols in order to highlight its features and we provide a security analysis of the system. As an extension of this paper we have also implemented a data transfer mechanism along with network creation mechanism.

## Keywords

Wireless Ad hoc Networks, Symmetric, Asymmetric, Secure Protocol.

## 1. Introduction

Spontaneous ad hoc networks are formed by a set of mobile terminals placed in a close location that communicate with each other, sharing resources, services or computing time during a limited period of time and in a limited space, following human interaction pattern [1], [2].People are attached to a group of people for a while, and then leave. Network management should be transparent to the user. A spontaneous network is a special case of ad hoc networks. They usually have little or no dependence on a centralized administration. Spontaneous networks can be wired or wireless. We consider only wireless spontaneous networks in this paper. Their objective is the integration of services and devices in the same environment, enabling the user to have instant service without any external infrastructure. Because

 

these networks are implemented in devices such as laptops, PDAs or mobile phones, with limited capacities, they must use a lightweight protocol, and new methods to control, manage, and integrate them.

Configuration services in spontaneous networks depend significantly on network size, the nature of the participating nodes and running applications. Spontaneous networks imitate human relations while having adaptability to new conditions and fault tolerance (the failure of a device or service should not damage the functionality). Methods based on imitating the behavior of human relations facilitate secure integration of services in spontaneous networks [3]. Furthermore, cooperation among the nodes and quality of service for all shared network services should be provided [4].

Spontaneous ad hoc networks require well defined, efficient and user-friendly security mechanisms. Tasks to be performed include: user identification, their authorization, address assignment, name service, operation, and safety. Generally, wireless networks with infrastructure use Certificate Authority (CA) servers to manage node authentication and trust [5], [6]. Although these systems have been used in wireless ad hoc and sensor networks [7], they are not practical because a CA node has to be online (or is an external node) all the time. Moreover, CA node must have higher computing capacity.

Security should be based on the required confidentiality, node cooperation, anonymity, and privacy. Exchanging photos between friends requires less security than exchanging confidential documents between enterprise managers. Moreover, all nodes may not be able to execute routing and/or security protocols. Energy constraints, node variability, error rate, and bandwidth limitations mandate the design and use of adaptive routing and security mechanisms, for any type of devices and scenarios.

## 2. Background Theory

Rekimoto introduced the concept of synchronous user operation in [8], and described a user interface SyncTap technique for spontaneously establishing network connections between digital devices. This method can deal with multiple overlapping connection requests by detecting "collision" situations, and can also ensure secure network communication by exchanging public key information upon establishing a connection. Shared session key for secure communication is created by piggybacking Diffie-Hellman public keys (generated by each device) on multicast packets.

These public keys are used to calculate a shared secret session key for encrypted communication. In this case, the authors do not propose any secure protocol. They have just added an existing security mechanism in their authentication phase. It is similar to the one used by us when a new node joins our network, but we have added other security mechanisms in order to create a complete secure protocol for spontaneous networks.

Spontaneous networks are also special case of humancentric networks [9]. Cornelius et al. implemented and evaluated AnonySense, a general-purpose framework for anonymous opportunistic tasking and reporting, which allows applications to query and receive context through an expressive task language and by leveraging a broad range of sensor types on users' mobile devices, and at the same time respects the privacy of the users.

This paper does not tackle routing issues in spontaneous ad hoc wireless networks. A paper that presents a security protocol for routing purposes, based on trust, is shown in [10]. 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.

## 3. Proposed Algorithm for Secure Spontaneous Network Creation

Our protocol allows the creation and management of distributed and decentralized spontaneous networks with little intervention from the user, and the integration of different devices

 

(PDAs, cell phones, laptops, etc.).Cooperation between devices allows provision and access to different services, such as group communication, collaboration in program delivery, security, etc. The network members and services may vary because devices are free to join or leave the network. Spontaneous network should complete the following steps in order to be created [1].

## 3.1 Procedure for Joining a New Node in the Network

The below Flow chart represents the procedure for joining a new node in the network.

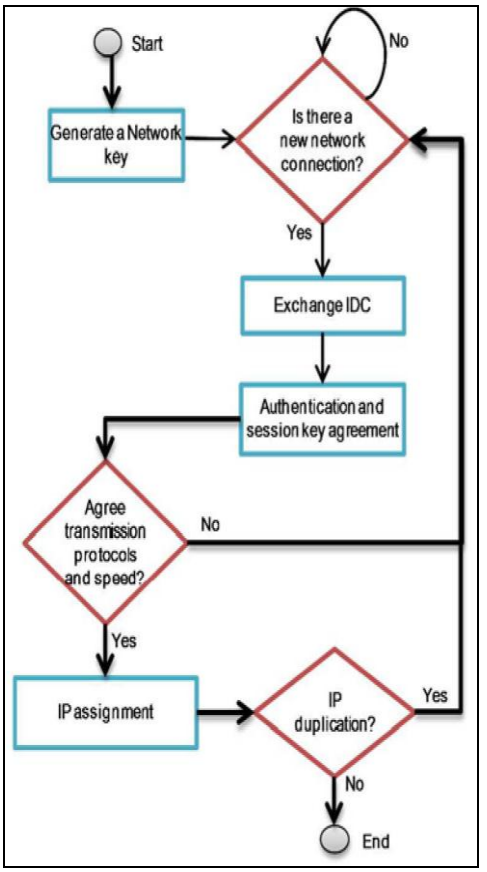


**Figure. 1. Algorithm for joining a new node**

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 (Ki), 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 (ki). 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.

## 3.2 Protocol Operation

In order to design the diagrams of the protocol, we have used the Unified Modeling Language (UML). The UML is a visual specification standardized language that is built to model object oriented systems. We use keys, activities, and use cases (diagrams offered by the standard) to define the processes, the structure of the classes in the system, and the behavior of objects or operations.
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, it begins the procedure shown in Fig. 2. First, a session key will be generated. Then, the node will start its services (including the network and authentication services). 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, the node follows Step 1 algorithm from Section 3, to find a device that will give trust to it, save corresponding data and will able to begin communications.

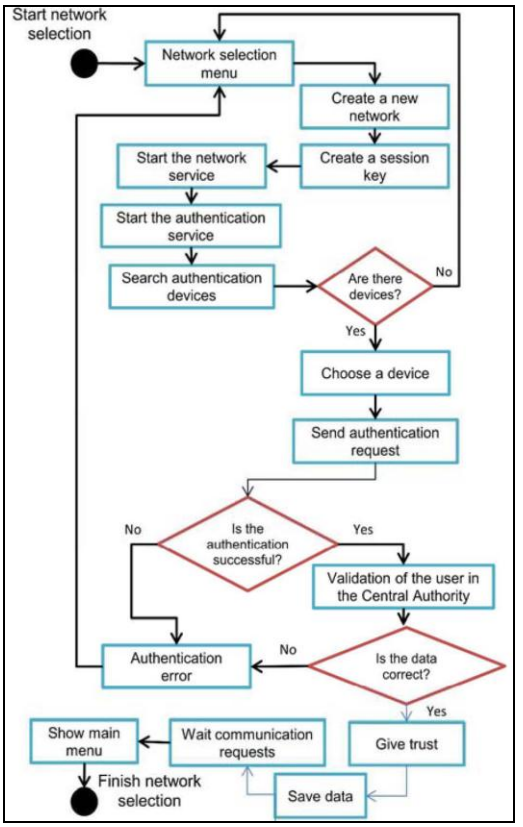


**Figure. 2. New network creation procedure**

## 4. Security Analysis/Evaluation of the Proposed Scheme

In this section, we analyze and evaluate the proposed security scheme. The proposed security protocol is adaptable because new security cryptographic algorithms can be easily added. In order to perform an analysis and evaluation from the practical perspective, we provide Table 1, which shows the most common attacks in spontaneous wireless ad hoc networks and how our proposal refuses them. We can observe that the secure mechanisms included in our spontaneous ad hoc network make it to accomplish high level of security.

**TABLE 1**
**Security Evaluation of Our Proposal**

| Attacks | How our proposal refuse the attack |
|---|---|
| Access to user date in physical device | User/password access<br>Privileges management |
| Compromised physical Device | User/password access<br>Visual identity verification (authentication phase) |
| Identity impersonation | Visual identity verification (authentication phase)<br>Use of short range technologies<br>Trust policies. |
| Phishing, active spoofing, compromised data | Hashing and authentication. Use of a trusted chain |
| Network data access using passive spoofing. | Ciphered using session key.<br>Key management |
| Access to network key using passive spoofing. (man-in-the-middle) | Asymmetric encryption.<br>Key-regeneration using trusted chains. |
| Access to private user delivered data using passive spoofing | Asymmetric or symmetric encryption guaranteeing confidentiality. |
| Data modification. Compromised data | Hash function to guarantee data integrity. |
| Lost data because of failures or battery discharge. | Persistent storage. Authentication. |
| Loose of connectivity. | Persistent data storage.<br>Authentication. |
| Overload and/or loose of resources. | Capacity plan and forecast.<br>Control the number of asymmetric operations<br>Persistent data storage. |
| Erroneous packets delivery | Control sent and received packets.<br>Packet retransmission. |
| Compromised node. | Use of algorithms to detect compromised nodes.<br>Change of trust level changed, trust elimination. |
| Data storage overload | Distributed data management and storage. |
| Denial-of-Service / Data availability | Distributed data management and storage.<br>Distributed access to data services. Distributed security processes. |
| Access to not reliable data.<br>Data disclosure. | Data access only through trusted nodes.<br>Session key regeneration. |

# 5. Proposed Implementation Modules

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective. The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods. The proposed consists of totally five modules:

1. Network Setup Model
2. Trusted User and node creation Module
3. New node Joining Module
4. New network creation module
5. Data transfer module

## 1) Network Setup Model

In this Module the user can register and login with the owner permission whether to join new node and or an existing node or to create a network. The owner provides session key based on the requirements of the trusted user.

## 2) Trusted User and Node Creation Module

In this module, the trusted user gets login by admin permission. The data is shared between two trusted users by session key generation for their respective data's and encrypting their files. The user can only access the data file with the encrypted key if the user has the privilege to access the file. Validation of integrity and authentication is done automatically in each node. And this forms a Spontaneous.

## 3) New Node Joining Module

By using Network based Intrusion Detection System (NIDS),the new node is created and they are joined to new nodes by respective procedures given by owner. The joining module is done with 3 phases:

### A) Joining Procedure

After joining the node, they are provided with IDC(Identity card and Certificate). IDC Contains both public key (user's information,IP) and private key(user signature).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. For eg. 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.

### B) Services Discovery

If a node asks for the available services. Services can be discovered using Web Services Description Language (WSDL).Our model is based on, but in our spontaneous network we don't use a central server. Moreover, other service discovery services can implemented in our system.

### C) Establishing Trusted Chain and Changing Trust Level

There are only two trust levels in the system. **For eg.** 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 behavior. Thus, node A may decide not to trust node B although A still trusts C and C trusts B

## 4. New network creation module:

In this module, we create a new network for the trusted users. The first node in the network will be responsible for setting the global settings of the spontaneous network. The second node first configures its user data and network security. Our protocol relies on a sub layer protocol **eg.**Bluetooth.After encountering the device, the authentication request is sent to another user. If authentication is accepted, it asks for data exchange .If failed the device wont exchange data.The authenticated node can perform the following tasks:

- Display the nodes.
- Modify the trust of the nodes and Update the information.
- Send data to all nodes
- Leave the network
- Process an authentication request etc., based on the a secure protocol for spontaneous wireless ad hoc.

### 5. Data transfer module

A node receives a data packet that is ciphered by a public key. When the server process received the packet, it is in charge of deciphering it with the private key of the user.

# 6. Conclusion and Future Work

In this paper, we show the design of a protocol that allows the creation and management of a spontaneous wireless ad hoc network. It is based on a social network imitating the behavior of human relationships. Thus, each user will work to maintain the network, improve the services offered, and provide information to other network users. We have 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.

As part of future work, we intend 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. The new nodes will not depend on a user, but on an entity such as a shop, a restaurant, or other types of services.

# 7. References

[1] L.M. Feeney, B. Ahlgren, and A. Westerlund,"Spontaneous Networking: An Application-Oriented Approach to Ad-hoc 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 andService-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 HocNetworks J., vol. 4, no. 5, pp. 567-585, Sept. 2006.

 

[8] J. Rekimoto, "SyncTap: Synchronous User Operation for Spontaneous Network Connection," Personal and Ubiquitous Computing,vol. 8, no. 2, pp. 126-134, May 2004.

[9] 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.

[10] 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.

## 8. About the Authors

**Botcha Sandhya Rani** is currently pursuing her 2 Years M.Tech (CST) in Computer Science and Technology at Andhra University College of Engineering, Visakhapatnam. Her area of interests includes Network Security, Parallel and Distributed Systems

.

**Sri.M.Sampath Kumar is** currently working as Associate Professor, in Computer Science and System Engineering at Andhra University College of Engineering, Visakhapatnam. His research interests include Cryptography, Algorithms, Data Security and Microcomputers.