An Overview on Working Principle of Spontaneous Wireless Sensor Network

M. Keerthika[1], M. Sheela Newsheeba[2], L. Gnanaprasanambikai[3]
[1, 2, 3] Assistant Professor, Dept of IT & CT
[1, 2, 3] Nehru Arts and Science College, Coimbatore.

Abstract- *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, where nodes can join and leave network and share or distribute information to each other like human communication model. As spontaneous network is self configured a security is a major concern. So a secure self configured protocol is required for user authentication, validation and data transfer. The existing system objective is the integration of services and devices in the same environment, enabling the user to have instant service without any external infrastructure. Secured protocol uses a hybrid symmetric/asymmetric key encryption scheme for user authentication and to exchange data. It is self configured as it is used to create and manage network, also manage resource sharing and providing services without any central infrastructure.*

Keywords- Spontaneous network, secure protocol, certificate authority

I. INTRODUCTION

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 neighboring 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.
The main features in spontaneous networks are the following.

- Network boundaries are poorly defined.
- The network is not planned.
- Hosts are not preconfigured.
- There are not any central servers.
- Users are not experts.

In this type of network the configuration services needed depend mainly on the network size, the nature of the participating nodes, and the applications that have to be carried out.

The spontaneous ad-hoc network is defined as a type of an ad-hoc network, which is formed during certain period of time with independent central server having no interference of an expert user, for carrying out any specific task or solving a problem. This network is built by numerous independent nodes coming together in the same place and at the same time to be able to communicate with each other. Nodes are able to enter and leave the network and they could be portable. When adjacent nodes discover each other within a short period of time, Spontaneous networking occurs. When a set of mobile terminals which are placed in a close location that interconnect with each other and also when one of the secure protocol which uses an hybrid symmetric/asymmetric scheme and the trust between users in order to share the initial data as well as to exchange the secret keys that will be used to encrypt the data, Spontaneous ad hoc networks are formed. Trust is based on the first visual contact between users.A Spontaneous ad-hoc network is a complete self-configured secure protocol which is able to create the network and share secure services without any setup. The network permits sharing resources and offering new services among users in a secure environment. The protocol contains all functions required to operate without any external support.

II. SPONTANEOUS WIRELESS NETWORKS

Although so far not as successful as managed wireless networking, an alternative type of wireless networks also emerged since 2000: spontaneous wireless networks. Inspired by the Push-To-Talk concept used in walkie-talkies (portable half-duplex radio transceivers developed during the

Second World War), spontaneous wireless networks depart from the traditional distinction between routers and hosts, whereby each user terminal (hereafter, node) may behave as a router and a host simultaneously. In spontaneous wireless networks, user terminals are thus "prosumers" (i.e. both producers and consumers) of networking resources instead of mere consumers. Terminals self-organize to provide multi-hop wireless communications among themselves, with or without help/control from infrastructure devices. Each node may thus simultaneously originate/receive traffic (role of a host), as well as forward traffic on behalf of other terminals (role of a router).

Popular examples of spontaneous wireless networks include mobile ad hoc networks, wireless mesh networks, wireless sensor or actuator networks, wireless smart meter networks, vehicular networks, opportunistic wireless networks or delay tolerant networks. Spontaneous wireless networks are considered as interesting solutions to extend and offload managed wireless networks hampered by increasingly heavy Smartphone data communications. They can also increase the resilience of the network in scenarios where infrastructure is not usable, due to a disaster, to the military situation or to the political situation, for instance. In addition, spontaneous wireless networking is an effective way to extend the reach of wireless Internet access, without costly additional infrastructure deployment .Popular link layer technologies providing device-to-device communication in spontaneous networks include so far IEEE 802.11 ad hoc mode and IEEE 802.15.4. However, in order to provide multi-hop communication in spontaneous wireless networks, additional techniques have to be employed on top of such link layer technologies. The focus is put on the use of standard IP protocols to enable multi-hop wireless communications in spontaneous wireless networks – in order for these networks to effectively blend in the Internet, where appropriate. Handling heterogeneity at layer 3 Since the early days of computer networking and the first steps of today's Internet, the diversity of networking technologies has been handled exclusively at the physical and the link layers (layers 1 and 2 OSI). The internetworking layer (layer 3) has been conceived as a "convergence layer" in which a single protocol (the Internet Protocol, IP) runs unchanged on top of heterogeneous interconnected networks.

The development of wireless technology entails however substantial changes in the way that networks are usually represented and conceived. Characteristics of spontaneous wireless networks cannot be handled exclusively at lower layers of communication, as they challenge some of the key assumptions of the IP based networking architecture. They need thus to be taken into account at layer 3. As more flexible wireless networks are deployed and get increasingly interconnected and integrated with other networks –or in the Internet–, the use of IP over these networks need thus to be adapted or reconsidered. The first contribution of the chapter is a review of these considerations, as it elaborates on how the IP-based network architecture.

III. SPONTANEOUS NETWORK PROPOSAL DESCRIPTION

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 the Device into the Network***

- Agree the transmission protocol and speed.
- Configure node addresses, routing information and other resources.

(2)***Discovery of the Services and Resources Offered by the Devices***

- Discover the services and resources shared in the network.
- Have a list of services and resources available in the network updated.

(3)***Access to the Services Offered by the Devices***

- Manage the automatic integration tasks and the use of, for example, agent service.
- Manage access security to the services.
- Manage the join and the leave of nodes of the network.

(4)***Collaborative Tasks***

- Within the intranet, among the various members.
- On the internet, with the other communities.

We emphasize that the main difference with ad hoc networks is that spontaneous networks are generated to work during a period of time on a limited space. Spontaneous networks are user-oriented and application-oriented networks that are based on human relationship and take into account the security and performance. A quick creation and configuration

of these networks will be fundamental to their performance. Feeney et al. explain the difference between ad hoc and spontaneous networks and, moreover, they identify five key challenges posed by the spontaneous networking environment. In our proposal we follow this because the devices have a similar behavior to human relationships. It lets a minimal intervention of the users and a quick configuration of the network and its security.

Many routing protocols for Mobile Ad hoc Networks (MANET) such as Destination-Sequenced Distance Vector (DSDV), Dynamic Source Routing (DSR), Ad hoc On Demand Distance Vector (AODV) and Temporally-Ordered Routing Algorithm (TORA) could be used in spontaneous networks. These protocols work with the concept of route discovery to locate the packet's receiver. In some cases, the protocols use caching methods to avoid looking for a route each time data have to be transmitted. We use this idea in spontaneous networks to improve the overload of the nodes, especially of those that act as gateways of the network.

IV. SECURITY IN SPONTANEOUS NETWORKS

Portable nodes that need to communicate during a reduced time slot for the formation of Spontaneous ad hoc networks. The problems of ad hoc network are similar to these networks, but increased because they are temporal networks formed in a given moment by a group of nodes that often users do not know each other. However, they must work together for the proper process of the network. Safe communication must be guaranteed with the help of cryptographic techniques. However, many of the outlined protocols assume that the nodes know the session key, when we talk about the use of cryptography of private key as well as the use of cryptography of public key. Methods to establish a safe and authentic communication channel is provided by these networks, assuming that the participants know the node which they are speaking with.

A fundamental topic in the environment of the security in spontaneous networks, when the nodes do not know each other and also the phase of connection establishment and initial exchange of keys. Security requirements in spontaneous networks and traditional networks are same: privacy, integrity, verification, no repudiation, and availability. Both data and routing information must be safe. The structures of ad hoc networks make these necessities much more difficult: dynamic topology, limited bandwidth, different capacity links and high error rates, energy and processing capacity limitations, absence of a central server, and often no prior information in the nodes to build the network.

The significance of the required configuration services depends on the size of the network, the applications to support it and the nature of the participants. Privacy, integrity, accessibility and control with verification must be offered without central administration and with energy limitations. Key generation, management, and distribution schemes that can be run on small CPUs are required by them. If we wish to create a spontaneous wireless network security comparable to the traditional networks two fundamental areas must be addressed. First, there must be atrust formation, key management, and membership control, and, second, there must be network availability and routing security. Our goal is to develop techniques in order to enable the creation of small- and medium-scale ad hoc networks based on the spontaneity of both. On the grounds of physical proximity, wireless connectivity is based; it reflects the ways human beings interact. People who are near each other can link, share things with each other, and ask people to relay information to others. This is all done with an appropriate level of security.

To get an appropriate level of security we establish numerous protection mechanisms as follows.

(i) Identification of the Nodes
(ii)Prevention of Proud Behaviour
(iii)Security in Routing Protocols against Manipulations.

V. AUTHENTICATE SPONTANEOUS NETWORK

A spontaneous ad hoc (or sensor) network enables a group of users to communicate and work together collaboratively very close to each other, sharing services, during a period of time. They seek to imitate human relationships in order to work together in groups, running on an existing technology. Devices used for spontaneous ad hoc (or sensor) wireless networks have limited resources, few computing capacity and low energy consumption. User-oriented and service-oriented spontaneous ad hoc and sensor wireless networks can be used to solve a problem, to carry out a specific task, or just to share services and resources between users, with no dependence on a central server.

The security protocol for routing purposes, based on trust that allows the Creation and management of distributed and decentralized spontaneous networks with little intervention from the user, and the integration of different devices is introduced by the flowchart that is shown below the creation overview of authenticate spontaneous network.

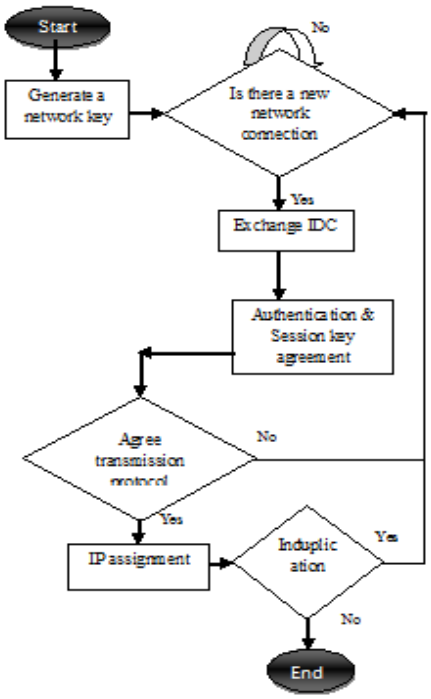

Fig. 1 Algorithm for joining a new node.

The following are the steps for Formation of authenticate spontaneous network.

Step1: Establishment

This step allows the 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 mechanisms. 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. It also contains the user's public key, the formation and termination dates, an IP proposed by the user, and the user signature. The user signature is created by 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. Then, the data summary is signed with the user's private key. The private module contains the private key. Phases of a node joining the network are: node verification 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 previous node. The public key is sent by the previous node A. Then, node B will send its IDC signed by node A' public key. The validation node received data and verification of hash of message in order to check that the data has not been modified id done by Node A. In this step, Node A establishes the trust level of B node by looking physically at it (they are physically close), depending on whether nodes A knows B or not. Finally, A node will send its identity card data to B node. This data will be signed by B's public key and will establish the trust and validity by integrity confirmation and verification. Others can access data,services, and B nodes certificates by a route linking other nodes in network, after the verification. 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 determinedly in the device for future use. No central certification authority is used to validate IDC. In each node validation of integrity and authentication is done automatically. The certification authority for a node could be any of the trusted nodes. The formation of distributed certification authority between trusted nodes is enabled by the system. When node A wants to communicate with another node B and it does not have the certificate for node B. it requests it from its trusted nodes. After attaining this certificate the system will validate the data; if correct then it will sign this node as a valid node. All nodes both clients and servers, can request or serve requests for information or authentication from other nodes. The first node creates the spontaneous network and creates a casual session key, which will be exchanged with new nodes after the verification phase.

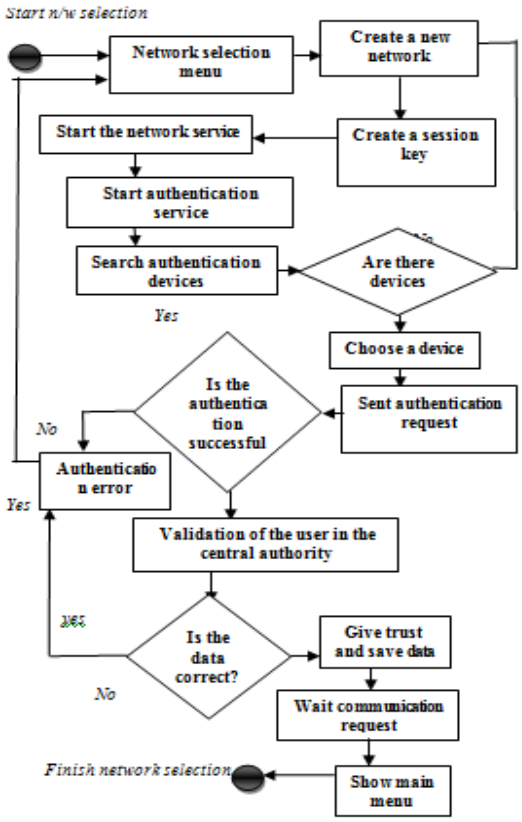

Fig.2 New network creation procedure

Symmetric key is used as a session key to cipher the confidential messages between trust nodes. It has less energy needs than the asymmetric key. It offers high safety because its design structure removes sub key symmetry. Further, execution times and energy consumption in cryptography procedures are suitable for low-power devices. The asymmetric key encryption scheme is used for distribution of the session key and for the user verification procedure.

The two types of asymmetric encryption schemes: Elliptic Curve Cryptosystem (ECC), because of its high performance cryptographic algorithm (RSA).After the mutual authentication, first node i.e. A will encrypt the session key with B's public key and will send it to B. The transmission of protocols and the wireless connection speed is decided by them. Lastly, node B will configure IP address and routing information. An IP address which has a fixed part in the first two bytes and the rest is formed by a random number which depends on the user's data is produced by B and secure routing protocol is borrowed from A. Formerly will send the data to procedure the routing information to A. Node A will check whether the IP is reproduced in the network. When B directs data to other network nodes A, e.g. node C, these data will be authenticated by C (using hashing and verification methods).By looking physically, later, node C will establish the trust level with B .If no trust level is recognized, it will be done afterwards by using trusted chains.

Step 2: Services Discovery

The accessibility of services is discovering by second node. Services can be discovered by Web Services Description Language (WSDL).Though our model is based on central server but in our spontaneous network we don't use it. For knowing the available services, a user can ask for other devices. It has a contract to allow access to its services and to access the services offered by other nodes. In such services a large number of parameters which are not transparent to the user and require manual configuration. One issue is to manage the automatic incorporation tasks and use, for example, service agents. The fault tolerance of the network is based on the routing protocol used between users to send information.

When node B leaves the network and disappears and also if there is a path to B only then the availability of services is provided to node B.

Step 3: Trusted Chain and Changing Establishment

Node A either trusts or does not trust node B.These are only two trust levels in the system. When it receives the authenticated Identity card from B, the software application installed in the device ask node B to trust A. Trust relationship can be asymmetric. Trust level can be established through trusted chain if A did not establish trust level with node B directly.e.g. If node A trusts C and C trusts B, then A may trust B. The changes in trust level can be over time depending on the node's behaviorist can also stop trusting if it discovers that previous trust chain does not exist anymore.

VI. APPLICATIONS OF SPONTANEOUS WIRELESS NETWORK

There is a wide range of environments in which these networks can be applied. This special issue tries to collect the most recent research of these types of networks .The permanently growing networked IT-infrastructure, the need for more mobility as well as the expansion of computer-aided applications to new areas demand new methods to simplify the handling of IT systems. Spontaneous networking is a means for simple integration of devices and services into networks. It seems to be one way to achieve more flexibility, more mobility, a better usability and less administration effort. It takes a closer look at the evolving technologies Jini (Java intelligent network infrastructure), JetSend, Inferno/Limbo, HAVi (Home Audio Video interoperability), and UPnP (Universal Plug and Play).

VII.CONCLUSION

In this paper, set of mobile terminals which are placed in a close location that communicate with each other and it is a complete self-configured secure protocol which gives more trusted way to spontaneous ad hoc network with every node maintain the network, improves the services offered, and provide information to other network node for the Formation Spontaneous ad hoc networks. We can add some new features to the user application, to the protocol and access control list.

REFERENCES

[1] S Preuß, CH Cap, Overview of spontaneous networking-evolving concepts and technologies.*Rostocker Informatik-Berichte* (Fachbereich Informatik der Universit at Rostock, 2000) 24, pp. 113–123

[2] S Gallo, L Galluccio, G Morabito, S Palazzo, Rapid and energy efficient neighbor discovery for spontaneous networks. Proceedings of the 7th ACM International Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems, October 2004, Venice, Italy

[3] LM Feeney, B Ahlgren, A Westerlund, Spontaneous networking: an application-oriented approach to ad hoc networking. IEEE Communications Magazine 39(6), 176–181 (2001).Publisher Full Text

[4] rking: an application-oriented approach to ad hoc networking. IEEE Communications Magazine 39(6), 176–181 (2001).Publisher Full Text
[5] CE Perkins, P Bhagwat, Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers. Proceedings of the Conference on Communications Architectures, Protocols and Applications (SIGCOMM '94), August 1994, 234–244
[6] DB Johnson, DA Maltz, J Broch, *DSR: The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks, Ad Hoc Networking* (Addison-Wesley Longman Publishing, Boston, Mass, USA, 2001)
[7] http://www.sics.se/~lmfeeney/publications/Files/wmcsa00 spontaneous.pdf
[8] http://www.ijert.org/browse/volume-2-2013/november-2013-edition?download=6753%3Anode-authentication-in-spontaneous-wireless-ad-hoc-networking-survey&start=620
[9] http://jwcn.eurasipjournals.com/content/2010/1/232083