EURASIP Journal on Wireless Communications and Networking
a SpringerOpen Journal

RESEARCH Open Access

Internet of things: where to be is to trust

Raquel Lacuesta[1*], Guillermo Palacios-Navarro[2], Carlos Cetina[3], Lourdes Peñalver[4] and Jaime Lloret[5]

Abstract

Networks' creation is getting more and more required, anytime, anywhere. Devices that can participate on these networks can be quite different among them. Sensors, mobiles, home appliances, or other type of devices will have to collaborate to increase and improve the services provided to clients. In the same way, network configuration, security mechanisms establishment, and optimal performance control must be done by them. Some of these devices could have limited resources to work, sometimes even resources restriction not existing, they must work to optimize network traffic. In this article, we center our researching on spontaneous networks. We propose a secure spontaneous ad-hoc network, based on direct peer-to-peer interaction and communities' creation to grant a quick, easy, and secure access to users to surf the Web. Each device will have an identity in the network. Each community will also have an identity and will act as a unity on a world based on Internet connection. Security will be established in the moment they access to the network through the use of the trust chain generated by nodes. Trust is modified by each node on the basis of nodes behavior.

Keywords: Internet of things, Trust, Network, Internet, Security

Introduction

In one way or another, when we talk about Internet of Things (IoTs) we should think that everyday object that surrounds us could be a proactive actor. Each node, such as fridges, mobile phones, cars, food, plants, or people needs a unique identification in the networks that let identify them when interacting with others. In addition, they will need an identity when connecting to Internet. Nodes will collaborate to provide security. Services such as privacy and authentication will be distributed among the different nodes depending on the node and the network status. A user could interact with house elements, with providers, a hospital, and others. Under this scenario, heterogeneous systems will be able to collaborate to provide services and data to users. As we work with ad-hoc networks, the identification and computation possibilities of all elements will provide a qualitative and quantitative leap in all type of sectors.

On the other hand, we should think about resources optimization. In a usual scenario not all of nodes will need to connect to Internet and to provide the same data and services. In some situations, one could provide other nodes connection and data if necessary. In this case, we work with communities. We will consider a community when several nodes work together to get a final goal. Normally, social networks are considered to be structures (often represented in graph forms), in which nodes represent individuals and connecting lines represent relationships among them. In such social networks information, friendship and other types of exchanges are carried out; this also being the means in which different people interact. Generally, society consists of individuals; however, these individuals tend to group together into communities. A community is a group or set of individuals who share common features: language, customs, values, etc. This concept of community might be considered similar to that of Virtual Organizations (VOs). However, a VO is usually related to business. Organizations created this concept to define adopted decentralized, team-based, and distributed structures. It was mainly due to the advances in communication technologies, which have allowed organizations to acquire and retain such distributed structures by supporting coordination among people working from different locations.

Some authors [1] had previously define the concept of Virtual Team as "a group of people who interacts through interdependent tasks guided by common purpose" that "works across space, time, and organizational boundaries with links strengthened by webs of communication

* Correspondence: lacuesta@unizar.es
[1]Department of Computing and Systems Engineering, University of Zaragoza, Ciudad Escolar s/n, 44003, Teruel, Spain
Full list of author information is available at the end of the article

technologies". A Virtual Team [2] is an evolutionary form of a network organization made possible by advances in information and communication technologies. The concept of Virtual Team involves permeable interfaces and boundaries, project teams that quickly form, reorganize, and dissolve when the needs of a dynamic market change, and individuals who are located all along the time, space, and cultures. In [3], a VO is defined as a geographically distributed organization whose members are grouped by a long-term common interest or goal, and who communicate and coordinate their work through information technologies.

This term is more similar to our term "communities". However, to create a "community", several groups (one on each physical location) are created. They do not work as individuals on a team but as a group on each location. The term "community" also will let work with individuals going further and trying to optimize resources on each location, as well as on the global group.

Communities often generate a common identity through differentiation with other groups or communities (generally common symbols or behaviors) which are then shared and developed by members. By and large, the formation of a community is motivated by a common need or objective (e.g., a common goal), though this is not strictly necessary, and a common identity may be enough to form a community without needing a specific goal.

Most of applications which have been developed for Internet users in order to interact socially have focused on developing relationships among them as individuals, assuming that every single person has the same technological resources and formats necessary to access the World Wide Web (WWW). This is not always the case; we will work with communities that shared Internet access to improve the use of resources as well as a better collaboration.

In our proposal, we use trust chain and communities to generate security access and distributed services. A node will not delegate all communications to routers. To optimize resources one node or several ones will be in charge of Internet connection, and they will send global data through Internet only when required; for example, in case of working in social groups (when a node need to send the common data), or because of necessity (existing nodes without connection). Those nodes that have Internet access or those that are in charge of this type of communication will send community data connecting themselves through TCP/IP protocols. A typical example is the electrical appliances in a house. A network is created, but not all the nodes should send Internet data. Only network status must be sent to inform. In this case, a node could be in charge of Internet communication (not always the same node, it will depend on the trust chain). Nevertheless, if two nodes are able to do it, both of them could do the work depending on the trust chain established (how the different nodes trust these nodes). In social networks, it is even clearer. When a node has better communication abilities than others, it can help other nodes to communicate. If a group of people is working to carried out a task, only one of them is required to send the common data to the global network. It is the same in a queue (a vehicles queue or even a people queue), where the main goal deals with informing to people/vehicles that are closer, so an Internet connection will be not necessary. However, we could report it to a global system. In this case, it will not be necessary all nodes to inform. Only several of them could be in charge of doing it.

This model could be applied to all type of devices. As a mater of fact, benefits of connecting Wireless Sensor Networks (WSN) and other IoTs elements go beyond remote access, connected among themselves (as heterogeneous information systems let them to collaborate) providing common services and being able to access and to carried out those that cannot be done by themselves. In a traffic jam, pedestrian mobile phones could communicate to estimate the number of people waiting on a traffic light (using sensors or identities) whereas cars' devices could estimate the number of vehicles waiting on the same traffic light. Both groups could communicate to the traffic light control server through Internet. The system could optimize the "changing of lights" of traffic lights of a zone via these data and not all devices need to send Internet data to the servers. This is a global example. Our proposal begins by establishing small or medium nodes to work.

Spontaneous networks

A mobile ad-hoc network is a group of mobile and wireless nodes that cooperatively set up a network without the support of any centralized infrastructure. If our network covers either medium or large areas, the necessary connectivity could be obtained using an ad-hoc routing. The required configuration services would be very significant depending on the size of the network, the nature of the participants and the applications that it supports. To characterize these networks, we enumerate a set of properties well known in the literature [4] affecting organization, operation, and management:

- *There is no fixed topology*: the devices are mobile and may move around freely in and out of each other's range.
- Each node is a router.
- Limited resources include CPU, memory, and energy. Mobile devices generally operate on battery power, which is exhaustible and the amount of energy available for each device may vary.

- *Shared physical medium transmission*: The transmission medium is accessible to anyone in range with the appropriate equipment.
- *The different identities are given by IP addresses*: each address is obtained dynamically, and therefore it is difficult to associate a fixed identity with an IP address.
- *Physical vulnerability*: the small size of mobile wireless devices means they can easily be stolen and possibly modified. Consequently, the relation with the owner node is not stable, the node may be subverted.
- *Lack of central administration*: The devices to be connected can come from anywhere and there is no central administration.

Feeney et al. [5] explain the difference between ad-hoc and spontaneous networks. Moreover, they identify five key challenges posed by the spontaneous networking environment. One of the main issues which makes a difference between the spontaneous network and fixed or mobile networks is that they facilitate the integration of services and devices, setting up both new services and configuration parameters of devices. It has to be done without the user intervention or interference in the operation of the network. The malfunction or failure of one of the devices or services does not compromise the viability of the community. Any resources being used by the community which malfunction are automatically released and the service is de-registered. Latvakoski et al. [6] proposed a communication architecture for spontaneous systems which integrates application-level spontaneous group communication and ad-hoc networking altogether.

Mani et al. [7] proposed SCOPE: A Prototype for Spontaneous P2P Social Networking. It provides customized social networking application for local use cases. Below the network level, SCOPE relies on 802.11 ad-hoc mode and needs no infrastructure. SCOPE follows the hierarchical P2P model. Some nodes with higher computing capability become super-nodes. Super-nodes form an overlay and provide the distributed data management system for the P2P social network. Client nodes connect to super-nodes and rely on them for sharing their contents or accessing to the shared information.

A spontaneous network merging is studied in [8]. The authors propose a novel approach for implicit merging of spontaneous networks following a group mobility mode. The inter-cell routing protocol avoids bottleneck links by geographically spanning the attribution of relay nodes to nodes willing to communicate with a node in a different cell. Former hierarchical routing protocols are based on the election of a cell cluster-head (or landmark node). A study (An Awareness Framework for Collaborative Spontaneous Networks: AWISPA) of the awareness in collaborative learning environments based on wireless spontaneous networks is carried out in [9]. A spontaneous network is created when a group of students come together and use wireless computing devices in order to carry out a collaborative activity. For the evaluation process, they first evaluate if AWISPA covers the requirements for support awareness in a collaborative synchronous application and second if a developed application based on AWISPA covers awareness in a real session with two groups with people collaborating among them. In both groups, they made a questionnaire analysis and found that the application fulfills AWISPA and therefore provides awareness.

Spontaneuos networks help us to generate working groups and virtual communities to work in the IoTs world. These networks are user-oriented and application-oriented and take into account the security and performance. Many routing protocols for Mobile ad-hoc NETworks (MANET) such as Destination-Sequenced Distance Vector (DSDV) [10], Dynamic Source Routing (DSR) [11], Ad-hoc On Demand Distance Vector (AODV) [12], and Temporally-Ordered Routing Algorithm (TORA) [13] could be used in spontaneous networks. These protocols work with the concept of route discovery to locate the packet's receiver.

Keys' generation, management, distribution schemes, and the different types of services that the network needs will be managed by spontaneos networks. Services as confidentiality, integrity, availability, and access control with authentication will be offered *without central administration and with energy restrictions*. Also the process is distributed in order that devices with small CPUs can belong to and participate. These groups will work in a collaborative way to provide security and tasks development. When the group needs to communicate through Internet, only several nodes (the best ones) carry out these tasks. Best nodes will be selected depending on capacities and trust chains generated. First node trust value will be established on the first contact with the device and it will be based on human relationships.

As a result, two fundamental areas must be addressed if we wish to create spontaneous wireless networks to let collaborative access to the IoTs. The first one deals with *network creation, trust establishment, key management, and membership control*; the second one deals with *network availability and cooperative work*.

Our proposal in spontaneous networks will be based on the establishment of trust chain created by spontaneity of human interactions. That wireless connectivity is based on physical proximity, reflecting the way *human beings interact*. People who are close to each other can communicate, exchange things, and ask people to relay information to others. In the same way, devices will

establish initial trust to other devices based on companies, under prior collaboration or other parameters. In our proposal, human beings can establish main trust value on a first interaction, previously and before the network is created. It is the pre-authentication phase. Services will be offered to other nodes by sending xml files with the necessary configuration data. Internet access will be carried out by those nodes that after merging the trust chain of different nodes, results in being the best ones. Moreover, they must have good communication capacities and offer these services. In our model, we trust nodes in order that we suppose they are going to offer those services they can provide, establishing they are not selfish. We will change the trust basing the new value on nodes behavior. We calculate it measuring different aspects of trust that we will evaluate on next sections. This is all done with an appropriate level of security. Within the network, each device will have a unique identification, and the network will also have unique group identification.

Our proposal has been developed with the main objective of improving the communication and integration among different ad-hoc networks (communities) having low resources. The collaboration among nodes will let all nodes Internet access optimizing network resources. Sometimes the cooperation will be necessary, for example, on rural or poor areas where not all devices are able of getting a connection to the network. In other scenarios, network optimization will be the main goal. We could cite several examples such as wireless sensor networks, mobile equipments, RFID tags, home appliances, cars, and many other daily objects that talk to each other, exchange information, generate aggregate knowledge and allow to quickly developing new advanced services for the final user.

Possible scenarios could be developed not only with wireless networks, but also with wired networks as electricity networks. In this scenario, sensing, computing, and web technologies converge and interact with each other. We will center our proposal on wireless networks. We have presented in Section 1 several scenarios where we can work with our model: people teams, wireless sensor networks, vehicular networks, etc. The work will be aligned to two use cases:

(1) Collaboration on educational environments in non-developing countries.
(2) Three companies in which employees meet to work together in different locations.

Spontaneous network proposal description

When several nodes wish to build a spontaneous network, they must meet in a physical location at a given moment. Concerning our use cases, one person arriving before a meeting to work collaboratively, for instance. If two people arrive together one of them must establish the network configuration.

First node that arrives to the place will generate the network configuration data. Second node will ask for the data to this node. Several networks could be created on a specific moment. If we want to work on two different networks (different work team), two nodes must generate both network configurations. Users will decide the team they want to participate in. Nodes willing to be network members first have to decide which network wish to collaborate with. Second, they will have to establish communication with a member of this network who after a pre-authentication will send the network data to this coming node. This will be the moment when first trust value will be established. Although it will be explained later on, we want to introduce how this process is done: employees belonging to the same company will establish (usually) trust among them. Students will establish trust on those classmates they trust. Teacher will establish trust among themselves and also on the students they trust. Third, the coming node will configure node addresses, routing information, and other configuration data and it will begin to participate in the network as a member. These data are sent on the pre-authentication process by the node that has generated the network. The collaborative tasks will be carried out within the intranet, among the different members and on the Internet, with the other communities. One team, the created in a city (City A) will be called for example “Community X Group A”. Team’s members are those working together in a physical location. On our use cases they will be for example people attending a business meeting or the people (student and teachers) that are together in a physical location. Another team, in other location, will be called for example “Community X Group B”. Sometimes teams could need exchange data. Teams are able to collaborate if one node is authenticated on both networks.

The discovery of services will be done through xml files. A node asks about resources and services offered by other devices and provides its main services as well as a resources list. In order to use services such as group communication, cooperation on running programs, security, etc. The members who make up this community may vary at any specific time (users may join or leave at will). Individuals will offer services to the rest of individuals of their group (data, reports, services, material to study, questions, and answers). A team will offer services to another team, for example, reports, common decisions, statistics, or others. In a classroom environment, they can give a lesson by video conferencing, doubts to be solved, exercises, etc. The node in charge of providing connection will send an xml file with all services offered by its group (added material, services, or others).

As presented in Section 2, there are several routing protocols for spontaneous networks. In some cases, 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 nodes, especially of those that act as gateways of the network.

A spontaneous network enables a group of devices to work together collaboratively while they are located very close to each other with a minimum interaction. It can be used for sharing resources and Internet services. Community lets several groups work together. Nevertheless, we should take into account resources limitation (of devices). Some users could work with mobile phones for example. Just one of the nodes has to be connected to Internet to share its connection and its resources to the whole network. Shared services are demanded in order to avoid nodes overload. Moreover, configuration with a minimal interaction from the user and security on the communication should be established. There are many application areas for ad-hoc spontaneous networks: industrial (communication among sensors, robots, and digital networks), business (meeting, stock control...), military (hard and hostile environments), and teaching. The range of environments in which these networks can be applied is wide and may include conference services and other "ubiquitous computing" applications at home or at the office.

A quick creation and configuration of spontaneous networks will be fundamental to their performance. In our proposal, devices have a similar behavior to human relationships. This topic is introduced in Section 4, and it will let users a minimal intervention and a quick configuration of the network and its security.

This article also shows the design and simulation of a model that lets optimal spontaneous network access using shared services. We present the procedure of the nodes involved in the system, where communities are created choosing the best node to be connected to Internet and to be communicated with other communities. Also, security algorithms are implemented. Moreover, we included the analytical proposal and its comparative with the most similar protocols in the literature. Validation of the protocol is carried out through several simulations and comparisons with regular architectures. The proposal has been developed aimed at improving communication and integration between different study centers of low resources communities but can be used in any situation where nodes collaborate to provide data.

Network auto-configuration proposal

When talking about IoTs we should think on that everyday object surrounding us could be a proactive actor. Nodes such as fridges, mobile telephones, cars, etc., need an identification that identifies it on their interactive communication and also when they connect to Internet. Moreover, when the devices join a network, they must have to be aware of all the different tasks needed to communicate with each other and the configuration of both logical and physical parameters (all of them should be automatic) [14], establishing the first value of trust. Users bring their resources to the system.

If we want to work with the community, at least one of the users of the spontaneous network needs to have Internet connection. The connection will be shared and that device will be the one that provides the access to the WWW (it could be applied to other services such as email, file sharing, etc.). There could be more than one Internet access in the spontaneous network and each one could share different services.

If none of network devices have Internet connection it will not be possible to collaborate on the community in a synchronous way. The work carries out by this team will be sent to Internet when the device, in charge of sending the data, can access to a connection. As a recommendation, at least one user having an Internet connection will be necessary on each team. It will guarantee an effective and right community work.

In this model, a user contributes capabilities, technical resources to access external services, and other applications (reports, exercises, games and other data which they may wish to share). The intranet and its view to the outside world permit the community both internal and external cooperations.

Resources of devices can also be used according to their available capacities. One user may be responsible for processing a specific task if another one needs to carry out this but does not find it possible owing to the fact that the device does not have enough resources. The following tasks should be performed when a user joins the spontaneous network:

1. Node identification.
2. Identification between nodes.
3. Trust establishment.
4. Address assignment.
5. Union to services.

These tasks should be carried out with a security mechanism. Consequently, when configuring an ad-hoc network, one of the main problems arising deals with the generation of a unique IP address. Most of the routing protocols assume that the mobile nodes are configured *a priori* with a unique IP address before becoming part of the network, which is not the case here. The problem comes from not knowing the topology of the network, neither when being set up, nor later on modification. A node may enter or leave the network at will at

any time, so a protocol must be capable of managing the generation of these IP addresses in order to run the network properly [15]. Also, the protocol must be able to detect the existence of duplicated IP addresses, which may occur, for example, when two subnetworks join together, or when a node which leaves one subnetwork with an IP (until then unique) joins another, or even when there is a substitution attack on the nodes. Some authors have solved this problem using DHT-based algorithms [14] as self-organizing systems and others use hyper cubes to implement indirect routing [16].

Faced with this challenge and after analyzing the working of ad-hoc networks, within the established framework, we propose a distributed and de-centralized solution (Figure 1).

Our proposal begins with the awareness that ad-hoc spontaneous networks need a flexible protocol which adapts itself to any number of different nodes and to their different characteristics. We could think on education collaborative environments in non-developing countries. People living there usually do not have devices with high resources and technology, connections have usually low bandwidth and not all people can access to it. In these places, the collaboration with developing countries could be really important to increase the development and educational level. Cultural aspects such a "language" could generate in this case the community.

In the formation of these networks a range of different devices (cell phones, PDAs, laptops, etc.) may take part. These nodes have to be configured in order to be part of the network. In spite of the fact that our networks do not include central servers, the operating of the wireless network must be similar to one with IP configuration infrastructure: translation of DNSs, service identification, etc. On the other hand, a minimum intervention of the user is required because it will be used by non-expert users, so the configuration must take place independently. The configuration of all the parameters necessary to form such networks implies an exchange of information among nodes.

In our proposal, we have designed a model where the nodes' IP addresses configuration has two main phases: first, a local connection address is generated by the node that wants to take part of the network. In order to generate the address we fixed the network identifier to a class B network that starts with 169.254 in IPv4 case. The same process is done with IPv6 (a link-local address is formed by using the well-known link-local prefix FE80::0). The rest of the IP address is formed by the chain of a random number of 4 bits in IPv4 case, that lets regenerate the IP if it has been duplicated, and 12 bits obtained from the 12 last bits of the obtained hash when we pass a hash function to the user's data. In IPv6 case, the number of bits is changed to generate same data. Second, we must check the IP duplication by one of the nodes that is already in the network. In order to perform this check, the node uses a broadcast technique that sends a packet with the proposed IP. If a node is using this IP, it answers to the new node. As the IP cannot be used by the new node, it has to propose a new IP. More details about the automatic configuration procedure can be read in [17].

Our approach is based on human relations. The set-up configuration is based on presentation or greeting. In a group of friends, a new individual is introduced to the other members by one of the participants. This member already knows the other's presentation data or may obtain it at the moment of presentation. He or she is then responsible for facilitating the new member's integration easily and simply into the group. On educational environments, teachers usually establish trust among themselves. New teachers will be introduced by those teachers

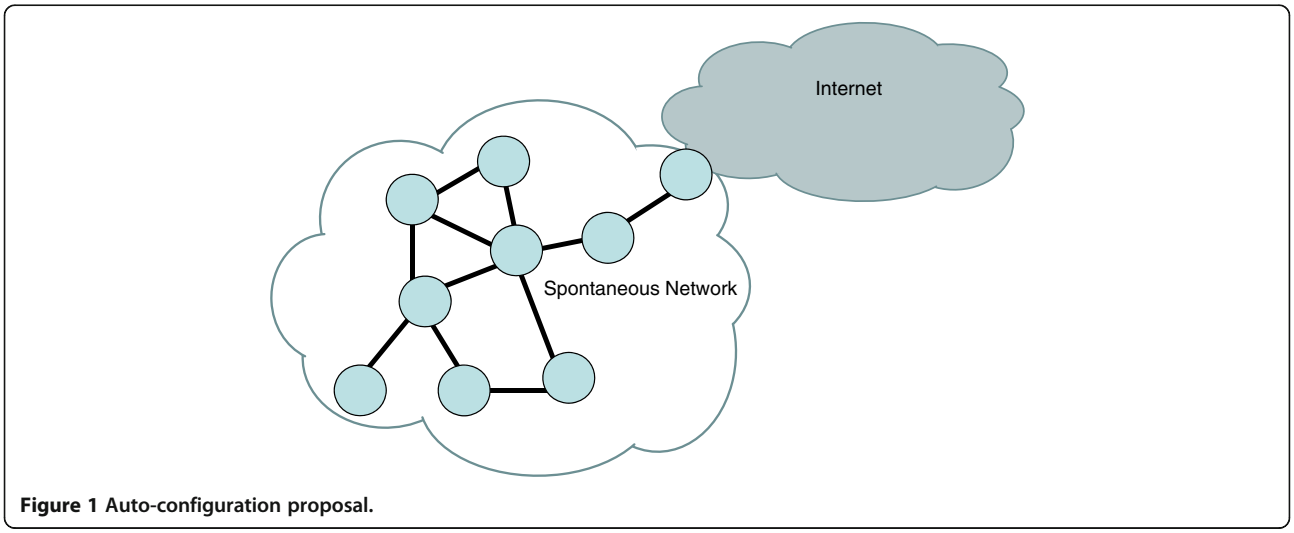

Figure 1 Auto-configuration proposal.

that personally know these new people. If nobody knows a person, trust will not be established. Consequently, the network management is built and run by cooperation among nodes, behaving similarly to human relations in our society. Thus, the formation of these networks is carried out in two principal phases: the first one is the presentation, greeting, or pre-identification and the second phase deals with the creation of the network and communication. As we can see in [18], the social relationship could be modeled as a spontaneous network. This has been the main reason to make a communication network based on this type of communications.

The presentation phase follows the human rituals enacted when different individuals come together to form a work group. This is carried out by one of the nodes already belonging to the network. In this phase, devices exchange the necessary information in order to be recognized; by presenting this information they gain access to the network. In this way, any user may come to be part of the network without having high level of computing knowledge. A user connected to the device has to insert his or her personal information when accessing the network for the first time. Automatically, a data configuration proposal is generated and available devices within range are identified. The intervention of the user is limited to select the user among those detected by the device and with which he or she wished to pre-authenticate. In the pre-authentication phase, the user also decides the trust level they have on the other user. A new teacher must carry out the authentication process selecting a device of one teacher he or she knows. If he or she does the process selecting other device, he or she does not obtain trust on the network. Trust could be obtained later, if the new device has a suitable behavior. We will see how trust changes in next section.

Once the device has been selected, the interexchange of presentation information takes place automatically between the two nodes; this information after being exchanged and authenticated, allows participants to gain access to the generated network and to establish the first value of trust existing among these users. In this network, each node acts both as a client and as a server, sending and receiving information and providing services to the other nodes in the network on request (e.g., PDAs, laptops, cell phones, among others). A device will receive the services offered by other devices, accessing to those it needs.

Trust must be established on an automatic way or previously by a user, company, or manufacturer if devices do not have a user that controls it. In the case of an automation system, the installer could establish trust among devices. In other cases, such a sensor that meets others a default value could be established. It could be changed by the performance processes of this node along the time. We work in this example with users with devices that meet each other.

In this scenario, the first node that creates the network is in charge of generating the "network data", which we could also call "community data". These "community data" will be sent to each node that be authenticated by one node that already belongs to the network. All nodes will work as everyday objects that surround us, they will become proactive actors, generating, and consuming information. However, when transferring data or services to other communities, we will not work with them as individuals, we will treat them as groups or communities (cars, electrical appliances...). All of them will have embedded computational capabilities and will work together to provide service on different sectors such as healthcare, logistics, automation systems, entertainment, and so on.

We can find some examples working now on IoTs in the CeNSE project by HP Labs, focused on the deployment of a worldwide sensor network in order to create a "central nervous system for the Earth", or the project "A Smarter Planet", a strategy developed by IBM which considers sensors as fundamental pillars in intelligent water management systems and intelligent cities [19]. At the same time, the technologies that will enable the integration are being developed and tested. The IPv6 over Low power Wireless Personal Area Networks (6LowPAN) standard, defined by Internet Engineering Task Force (IETF) [20], allows the transmission of IPv6 packets through computationally restricted networks. However, having IP connectivity does not mean that every sensor node should be directly connected to the Internet so security is becoming one the most challenges in this matter. In [21], the authors focused on one specific challenge: the actual connectivity model between the WSN and the Internet, trying to answer if sensor nodes should delegate all Internet communications to a set of central management systems, or should they become first-class citizens of the Internet by implementing the entire TCP/IP stack plus other standards like web services.

Establishment of trust chains

Concept of trust

Trust is a function of the amount and type of control one has in a relationship [12]. Social exchange theory asserts that individuals weigh the costs and rewards in deciding whether to engage in transactions. If the rewards are determined to outweigh the costs, then the individual is likely to enter an exchange relationship. Trust is critical for this process because it is believed to reduce the perceived costs of it. As we can see in [22], trends in persuasive computation are based on cultural and social knowledge. This knowledge will serve us to

establish confidence chains among devices. In our scenario, these devices will work with users.

Indeed, we use extrapolated mechanisms of human relationships to carry out device identification and user authorization. The formation of this type of nets follows the same patterns: presentation, exchange of greetings, etc. Thus, people located close can communicate with anybody; they can exchange information with each other as well as ask people to forward information to others. In particular, authentication and trust can be based on interaction at first hand, rather than being remote or by means of centralized administrative services. Later communication will not need direct contact. The model is implemented based on the idea of trust. This idea was already presented as a trust net [23], and we apply this idea in spontaneous and pervasive scenarios. Our protocol is based on the use of two information structures, an IDC (IDentity Card) and a certificate. Be i any network user, the IDC is formed by a public part: identity, public key of the user (Ki) and a data signature. Private part is formed by the private key (ki) (which is not accessible by other devices). A certificate of an i user could be signed by himself with his private key or by another user private key. When we obtain the certificate we can consider it "valid" if the signature of the data corresponds to the owner of the public key or to other user public key (on which we trust and has carried out this signature). If we trust the key we receive, we will sign it with our private key. We will consider it "trustworthy" if the owner is trustworthy. In other words, if he acts responsibly when signing keys. A signature from a reliable person allows a "net of trust" to be established among keys that have been distributed by non-direct means. Other nodes that trust us will be able to request a key. This method will allow data to be distributed. It means that nodes belonging to the net are often lost or abandoned or new ones may be included; in the latter case, the node that wants to be part of the network will have to be validated by the current network components.

If a new device is "introduced" to the net and does not have a private–public key, one must be generated, to perform authentication and to communicate in a secure mode with the rest of the nodes. Once this new node is admitted, it will need to know the "community data" to be able to communicate with the other nodes. By means of the public key it can obtain the key belonging to the network, generated by one of the nodes that already takes part of the net. If one node distrusts another, it will be able to revoke its permissions. If a node leaves the net, it can maintain the network data in case it wants to re-enter the same net. If more time than the session key expired time has spent, it will have to authenticate again.

A node does not have to obtain public keys for all the nodes that form the network. In other words, one node does not have to broadcast its authentication information to all the other nodes in the network. Nodes will be able to obtain the information in a decentralized and distributed way through "nets of trust" [24-27]. The administration of this trust will be based on criteria of "validity" and "trust" [28-30]. We will also be able to establish ranges of trust. Our key signatures will also be visible to other users. If they trust us, they will consider this key as valid, that is the same as a "net of trust" that will allow us to create a secure net.

Supposing one example in which the network consists of three nodes. Teacher 1 (node 1) and teacher 2 (node 2) know and trust each other. Then, teacher 2 trusts a third node, teacher 3 (node 3). If teacher 2 receives a public key from teacher 3, (trust node of it) and signs it with its private key, we consider that the owner of this key is "trustworthy". Later, if teacher 1 wants to obtain that key, it can be obtained from teacher 2, and since teacher 1 trusts teacher 2, it "validates" this new key too by signing it with its private key. If teacher 3 is not trustworthy, any key signed by this node will not be considered a trust key. Furthermore, teacher 1 will never sign teacher 3 key although it might forward it. To sum up, we can establish a distributed key administration service (Figure 2) through the use of a "trust net" based on the criteria of validity and trust. To set up the net, public keys only need to be obtained when necessary.

A node willing to access to services will ask for them to those nodes it trusts. When a community (a network) want to send global data, trust chain will be merged to detected those trustest nodes that also offer Internet connection. Values established initially among nodes will change throughout the time. New values will be established taking into account the behavior and operating of

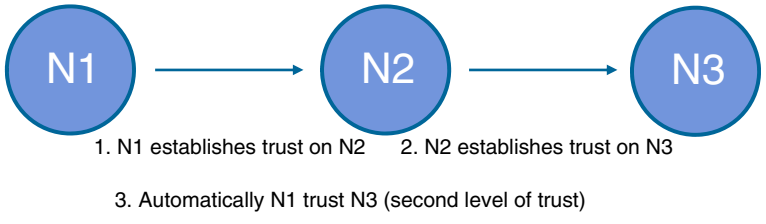

Figure 2 Establisment of trust chain.

the nodes in the network. Parameters to be borne in mind for the update will be discussed in Section 6.

Network performance

On our proposal the knowlegde of the network is based on several parameters:

- network configuration
- user configuration
- network inputs and outputs
- context
- type of required service

According to these parameters, network and nodes will establish both (a) network security level which is based on the trust network generated and (b) network performance level (see Figure 3).

These parameters let our net establish a balance between performance and security associated to the situation and the current scenario.

As an example we can show the following situation. Several users estimate that security level has to be high (e.g., on a meeting where companies' employees are exchanging confidential data or data about a new product). If these data are accessed by external users, the product or the company could lose its competitiveness. A laptops' network in a meeting is the context. Network configuration is HTTP and IPv6 protocols, working also with a common session key and user's keys. Inputs say that the network does not have bugs and nodes are confident. Outputs are a correct network performance. In this scenario, the network could decide that the required service needs high security. This high security implies the use of authentication, privacy, and integrity. Other inputs, such as compromised nodes detected, will imply also the use of trust routes (based on trust chain). In other cases, the use of the trust chain could not be always necessary. To implement the proposal, a relation among the items and the final security and efficiency need to be established.

Changing trust values: parameters to be taking into account

Trust value that one node has on another must not be fixed. These values are going to change all along the time. New trust values will be established taking into account several parameters. We present some of them. Once the node has changed the trust value of the nodes, it will send these data to the rest of the network nodes it trusts. Figure 4 shows the considered parameters.

Physical proximity

Sense of community has been all along the history a main point to establish trust. This trust is usually established due to dependency on proximity and common history. It makes a common identity.

In our model, face-to-face meetings are necessary to establish first values of the trust chain. In some other models (e.g., home environments), the company operator or even the house owner can decide how to establish first value of trust among home devices and also, among the community (created by the home devices) and the user's devices (mobile phones, laptops,. . .). Trust usually tends to particular nodes in networks: we should

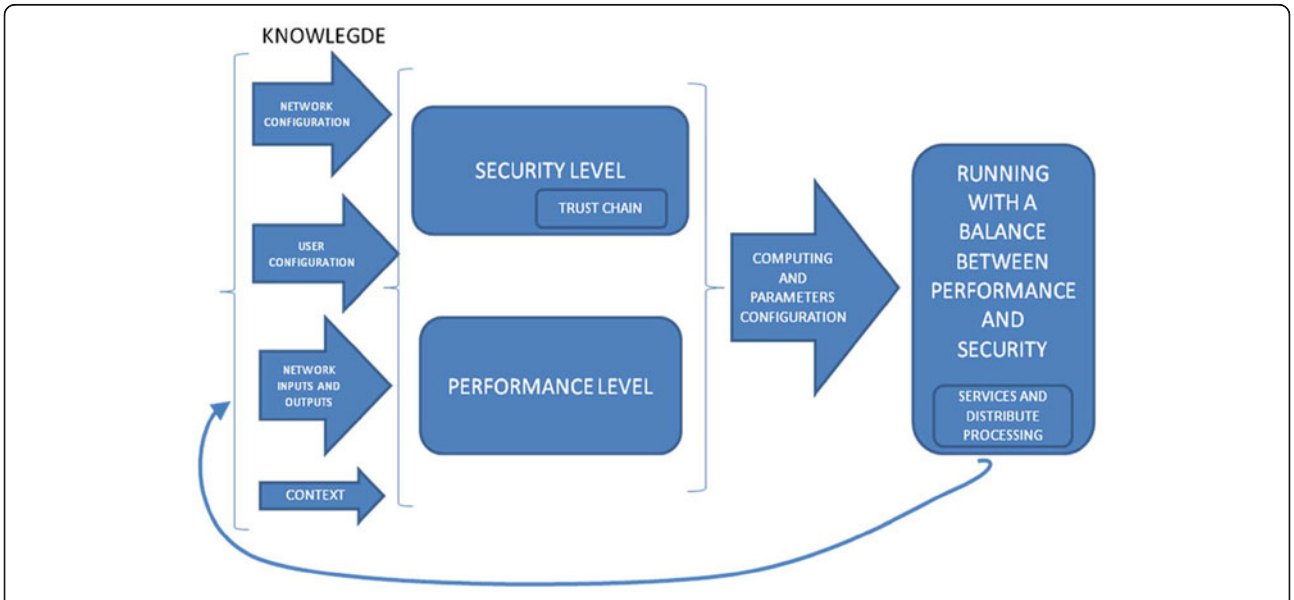

Figure 3 Network performance.

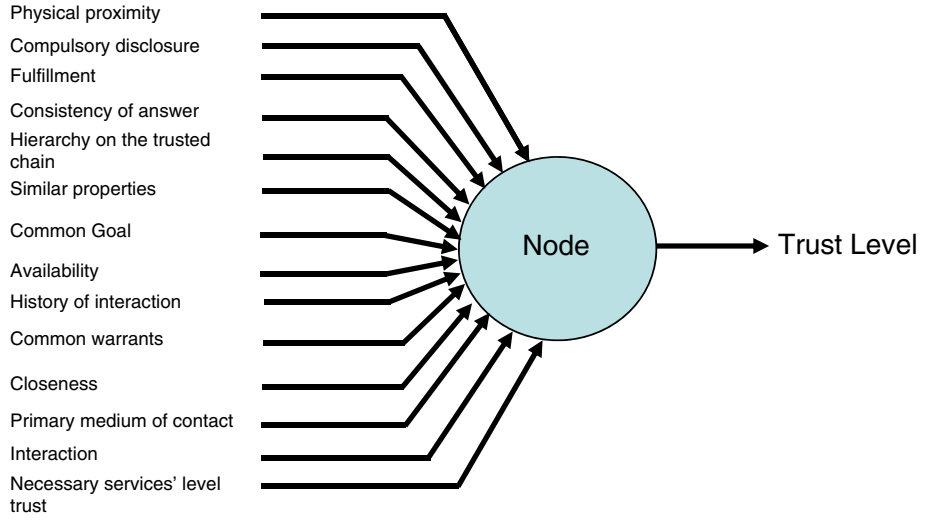

Figure 4 Establishment of trust value.

take care of attacks to these nodes. Although a node has few values of trust, the rest of the nodes could interact with it. It is only a question of security in the process. If a process requires a high level of security, it will be treated only by trust nodes. In automatic networks such as network sensors, we could establish more trust as fewer hops a node is from other. On educational environments, for instance, we could decide that trust is established over those teachers that work together.

Compulsory disclosure

This parameter is focused on past behavior on information disclosure. It is another factor that lets explore the concurrent influences of users' privacy perceptions and attitudes toward other users (nodes). Thus, it is necessary to explore the *quality* of information disclosure in the network. Characteristics such us regard for user, time of collaboration among nodes or previous behavior, making a node perceive privacy protection. The more time a node has been collaborated on a right way with other, the more trustworthy the node will become [31]. In the model, all nodes collaborate to maintain the security in the network. At specific intervals they send security data about network performance to other nodes. In this way, it is not necessary that all nodes verify all data. Benefits of providing information help to the relationships among them. It lets increase trust in nodes that provide us useful data. If a node has lack of trust it will be isolated as far as access to services is concerned.

Trust will be a key to engage in a transaction because it reduces the risks associated with access to services over both local network and Internet. These risks include theft of identity information among others. Trust usually increases confidence; a user prefers to do business with trust nodes they perceive to be reliable, honest, consistent, competent, fair, responsible, helpful, and altruistic (key components of trust). We apply these user's characteristics to nodes. The way of working will let establish them as trust nodes. The role of trust in data disclosure may be particularly important in networks where nodes have low resources. Typically, one will tend to trust (much more) those teachers that give him/her more useful information.

Fulfilment

An important requirement for a trust node deals with fulfilment. Nodes expect to obtain services efficiently and with minimal hassles. Security and routing data let users to access to data in a secure and private way. If fulfilment is not performed, other nodes will change trust on these nodes. A mistake could cause the user lose data or wrong information.

In these processes several criteria have to be evaluated: optimization, each node must be able to improve the network's global performance—no overload, a low bandwidth, a low number of messages—achieving also its goals. Furthermore, the necessary computing processes should be easily processed, without lack of reactivity. We define also a global trust level belonging to the network; it lets work with other networks (other communities) as a global entity. We should think that it happens usually (friends, global social societies, a house with different electrical appliances). It could work as a whole without necessity of individual trust entities. We will compute multi-dimensional trust values, to combine these values into a global trust level and to use this trust level to make decisions. Those devices offering us better quality of service will obtain higher level of trust.

Consistency of answer

Within an environment characterized by pervasive nodes, it will be necessary to provide verifiable proofs for claims related to authorship and integrity that would usually be taken at face value in the physical world. Fakes must be detected. Immediately, nodes must inform the rest of the network nodes. Integrity and authenticity will be directly related to questions about trust and identity in the network information world. We must examine the provenance of the object. The chain of routing has to be validated through an analysis of the documentation. Data have to be consistent with the claim made about the record of its provenance. Authenticity and integrity must be guaranteed by means of the use of signatures and hash functions attached to the object or the claim that comes.

Hierarchy in the trust chain

Trust, established directly by the user, will have a higher value than third trust nodes (established by your trust nodes). Each user will have a level of trust over the rest of users. Sometimes, he/she could receive a certificate from a node it trusts, but other times the user does not trust on the issuer of a certificate. In this case, it could be addressed in the certifying process by a hierarchy of trust.

A hierarchy of trust begins with at least one node a user trusts. This authority is called the root authority. The root authority then certifies other nodes, called first-tier certification authorities, who can then issue certificates and also can certify additional or second-tier certification authorities. The receiver of a certificate can determine whether the certificate's issuer is certified by a valid certification authority entity. That is, a node belongs to the chain of trust exists. A user could decide trust only several levels of trust chain hierarchy.

Similar properties (age, gender, type of sensor. . .)

Community and societies let establish mutual trust among individuals. They usually follow common goals that let join to work.

Common goal

When several nodes have common goals they try to collaborate to get them. Each node will have to design individual performance goals that emphasize both results and nodes common goals.

When one node is in the process of building trust, it helps to establish common goals at the beginning until trust is earned or regained. If networks do not run properly, it must be necessary to revise shared goals (e.g., getting the network back on track). It will be necessary to state the obvious, "none of the nodes wants to crash". For instance, it could be necessary to increase security level at certain moments to transmit secure data, but after this, the network should again come back to the previous state. On the other hand, network could be saturated by overload nodes. In this case, the common goal will be a secure transmission without security overload. Nodes have to establish their individual goals, but they should contribute to reach common goals. Similar objectives with other teachers could imply an increasing trust level on this teacher to improve results.

Availability (mobility)

Nodes must be available for services access; operation and use as committed or agree. If a node is accessible and is providing services and data to the network all along time, it could be considerate as more trustworthy than other nodes that move often. They let set a minimum acceptable performance level for system availability. The minimum performance level is established through commitments made or by mutual agreement (contract) between the parties. Those teachers that usually collaborate on more tasks will have higher level of trust.

History of interaction

Node trustworthiness can be determined by investigating the interaction history of the node. Data could be obtained from the own data or from other nodes if the end-peer has no previous interaction with it.

Common warrants

The process of negotiation defines security key size, protocols, and other algorithms to be used among nodes. Trust should be higher with those nodes that work with more secure and effective algorithms. If an employee decides that higher security is necessary, he/she only trusts those nodes working with the same security level.

Closeness

Both social and physical closeness usually can guarantee a better access to services.

Primary medium of contact

Depending on the first medium of contact of two nodes (long distance or short distance medium) we could verify more visual or other users' characteristics, we can also check the user as known.

Necessary services' level trust

It is not always possible to prepare training data consisting of users' location histories and user properties nor behavior of these nodes. We should find mechanisms to find out if a node has the level of trust necessary to interact with them, depending also on the services and security level required. Besides this, nodes usually change their position. Network behavior will have to adapt to these changes. It will be useful if we can know the usefulness

and trust of a node using location histories, own trust history, and third party trust history.

Interaction

A node that does not interact with others at all is almost useless, at least for network purposes. Therefore, a definition to measure the usefulness of a node deals with analyzing the total number of "right" interactions. The importance of a node is understood in our model as follows: the node performance becomes better than other node if they provide us a good connection performance, better data and more access to services and access to secure services.

Simulations

Simulations have been performed with Castalia simulator. The model uses trust net as a protocol to send messages among different nodes. We can simplify this with the following example. Given three people and two of them know a secret. There is only one possibility for the third person to know the secret: at least one of the two people trusts the third person. This simple example explains the concept of "Trust Net" and how we will exchange data among nodes.

The algorithm for spontaneous networks this model uses goes like this. During the start-up of a node the model broadcasts messages toward the rest of the nodes. This process is the same for every single node. A node accepts another node as its neighbor depending on how many messages the node received from another node. When a node has its trust network formed by all its neighbors, then it will start to send its own identity card toward all its neighbors. If the neighbor sends a message back which states that it has received the identity card and that this is correct by checking the hash, then the node trusts its neighbor. If a node trusts another node, then it can send messages directly toward it. If a node wants to send a message toward a non-trust node then it has to do this through a trust node. The modifications of node's trust value through the parameters introduced in Section 6 is not going to be addressed in this article, where only a theoretical analysis has been carried out. The following tests have been taken in an area of 1000×1000 m^2 (see Figure 5). The neighbor threshold is 95%. We can see that as the number of nodes increases, the number of neighbors increases. This is absolutely normal because there are more nodes closer to each other. Nevertheless, we can also see that there are no single nodes that can reach every neighbor. One of the main reasons deals with the size of the area as well as packet loss due to collision.

As far as the collision model is concerned, there are only two collision models included in Castalia. Castalia also considers two other collision models but they are not included in the current Castalia version (Castalia 1.3): (a) no collision, no interference, and (b) additive interference model, where transmissions are seen as interference.

This simulation has been tested within a 100×100 m^2 area. If data are sent to other nodes taking into account trust network, we can see that on the collision model (Figure 6) the two top lines are the average and the maximum number of nodes when there is no collision.

The other two lines represent the additive interference collision model. As one can see, there are a lot of

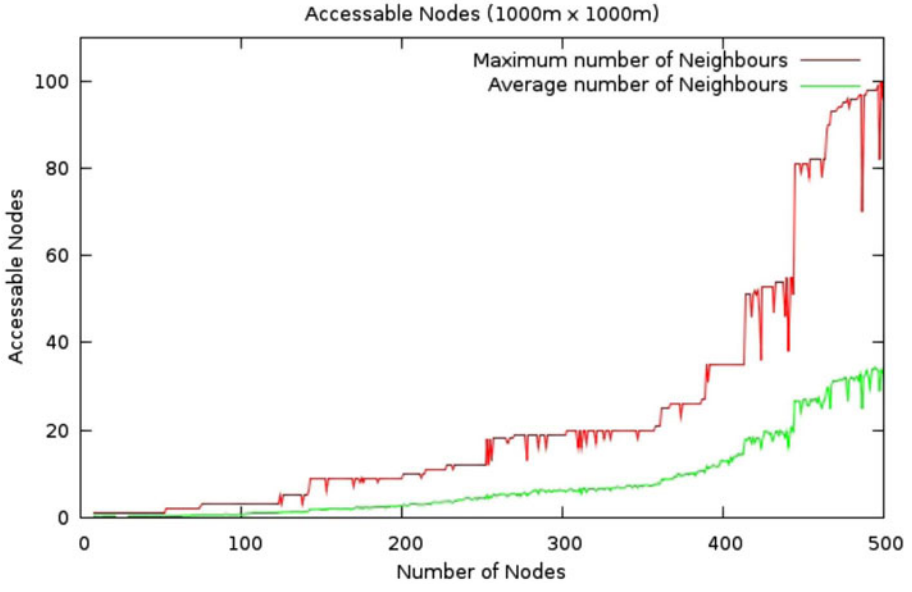

Figure 5 Simulations made with Castalia simulator within an area of 1000×1000 m.^{2}

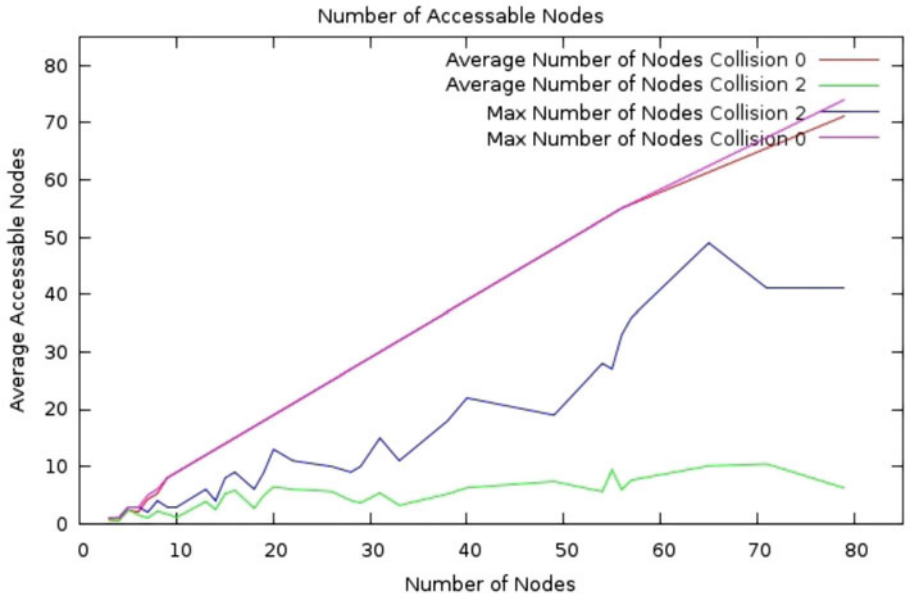

Figure 6 Average number of collisions in the trust network.

differences in the amount of neighbors between these two. Of course, if there is a collision, a lot of sent messages are lost and that is why there are fewer neighbors.

The following test will show us the difference in number of neighbors when we use different kinds of links. We will explain which the difference is among the three different lines. First, we have bidirectional links. Bidirectional links force links to have the same link quality in both directions. Second, we take into account unidirectional links. In this case, there is no correlation between the two directions and the fading is chosen independently. In fact, there is always a correlation between links in one direction and the opposite, but there is still a great variation. Third, we consider an ideal network. In this case, we have also bidirectional links but the sigma of the wireless channel is set to zero. This forces all nodes that are at the same distance from the transmitter to get the same signal strength. The bidirectional links are scoring the best on the amount of neighbors (see Figure 7).

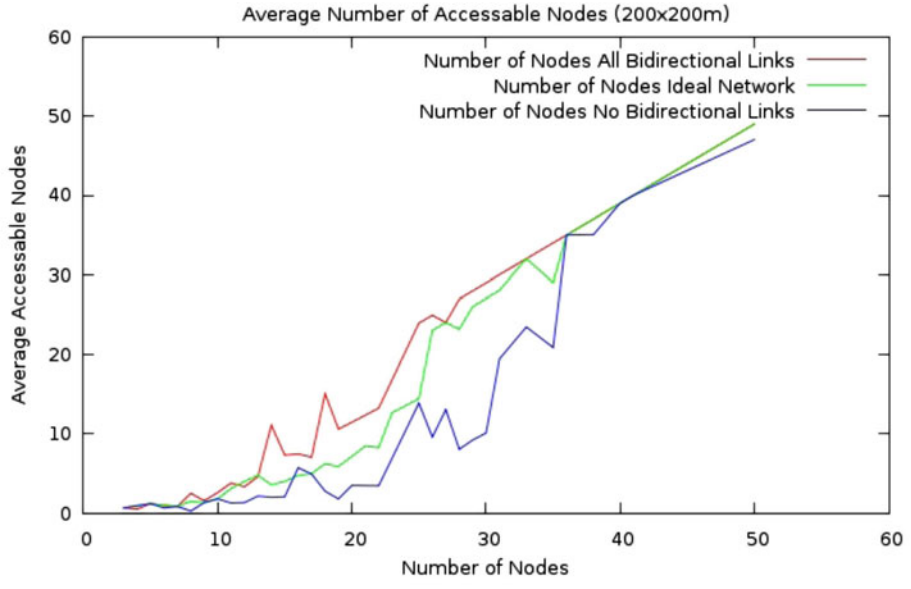

Figure 7 Accessible nodes in the trust network.

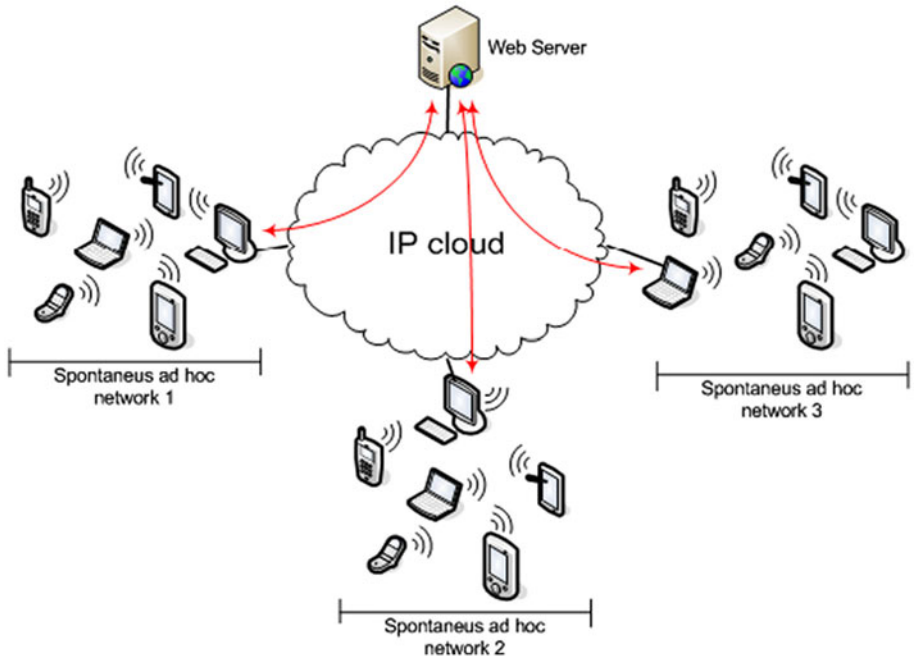

Figure 8 Simulated network diagram.

Model validation: test bench

First validation has been performed using OPNET modeller simulator. Figure 7 shows the diagram for the simulated network. In order to evaluate our proposal, we simulated two situations. On one hand, we use the architecture proposed in Sections 4 and 5, where nodes interact with each other and only with the node providing Internet access if they wish to communicate with this one or if they need to make an http information transfer to other communities. On the other hand, we use a conventional architecture, where each call to the network goes to a server and this server answers with the adequate content. OPNET modeller simulator has been used. With this tool we have created a situation in which there is a Web server connected to an IP cloud, which simulates Internet behaviour. Different spontaneous networks also connect up to this IP cloud, as seen in the diagram of Figure 8.

Each spontaneous network consists of five or six MANET devices. Nodes in the topology have the following characteristics: a 40-MHz processor, a 512-KB memory card, a radio channel of 11 Mbps, and 2.4 GHz as the working frequency. The network protocol running these MANET nodes is AODV. We selected this protocol because it possesses the best connectivity to Internet.

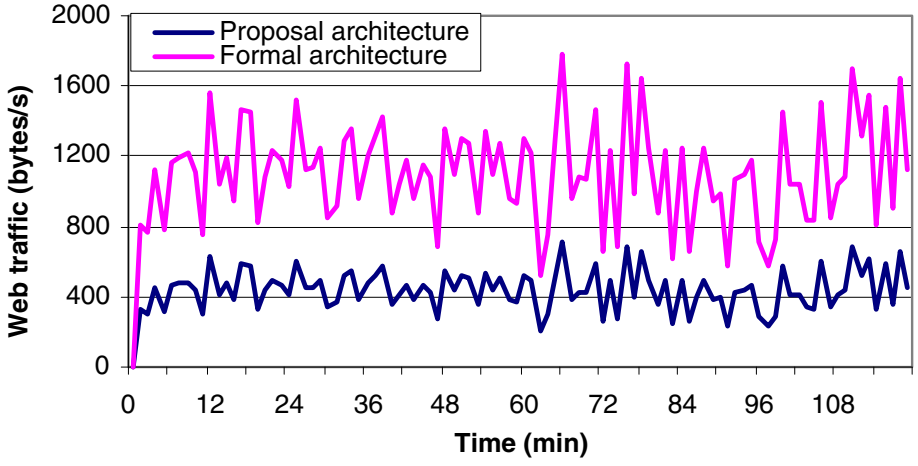

Figure 9 Web traffic circulating in the IP cloud.

Figure 9 shows the Web traffic circulating in the IP cloud of our simulation. We can observe the behavior of our architecture compared to a normal architecture. Note that the average Web traffic in our proposal is around 430 bytes, compared to the traffic when using a conventional architecture, where the average is around 1090 bytes. Therefore, a 61% improvement is displayed. What is more, we observe that in our architecture the traffic is more stable and displays fewer fluctuations.

Conclusions

Social networks are getting more and more important as a basis to establish trust chain among users. Each object establishes its trust chain basing on its trust nodes. It is important taking into account the social factor and that of personal relations as a starting point in the configuration of networks of devices, where these devices associate or interact finally with users. Chains of confidence will allow the establishment of groups or communities and unique identities (for the above-mentioned communities) for the access to services as well as for the spreading of group information. Thanks to the group organization we will be able to optimize resources, as well as to avoid the excessive multiplication of the transmitted information.

In addition, we have introduced the adjustment of these social chains to objects, as well as criteria to be valued to modify the trust along the operation of the network. Being in a scenario of spontaneous networks, so used nowadays, we have analyzed the transmitted traffic, being aware of the optimization that conformation of groups generates, as well as the variation in the confidence chains, establishing the closeness as a trust criterion.

Method

The methodology we have followed in the design of the secure protocol for spontaneous networks has been done on a waterfall cycle basis, pursuant to three basic principles which are common in this type of research activities:

1. Previous and continuous study, not only from the bibliographical point, but from the applications and real systems point of view.
2. Design of the model, study and obtimización of processes.
3. Development based on the creation of prototypes of simulation with cycles in spiral, through which software prototypes will evolve according to the following steps:

a) Development of a final prototype.
b) Validity of the prototype and that of the stipulated procedures. Measurement of the benefits and improvements obtained with regard to previous models, study of the network performance.
c) Adaptation of both the design and the model of simulation taking into account the observed measurements.

The final goal of the project deals with the validation of a system of secure spontaneous networks based on confidence chains. Obviously, to reach this aim, we have to go through the accomplishment of small-scale prototypes as well as through the accomplishment of simulations that allow us to validate the proposed schemes. The simulation phase is vital, especially in relation with the design of protocols, in order to guarantee a suitable operation of the above-mentioned models.

The proposed schemes will be evaluated using the Castalia simulator ((http://castalia.npc.nicta.com.au/).

Competing interests
The authors declare that they have no competing interest.

Author details
[1]Department of Computing and Systems Engineering, University of Zaragoza, Ciudad Escolar s/n, 44003, Teruel, Spain. [2]Department of Electronic Engineering and Communications, University of Zaragoza, Saragossa, Spain. [3]Department of Electronic Engineering and Communications, San Jorge University, Zaragoza, Spain. [4]Department of Systems Data Processing and Computers, Polytechnic University of Valencia, Valencia, Spain. [5]Department of Communications, Polytechnic University of Valencia, Valencia, Spain.

Received: 15 February 2012 Accepted: 14 May 2012
Published: 21 June 2012

References

1. Lipnack J, Stamps J: *Virtual Teams: Researching Across Space, Time, and Organizations with Technology*. New York: John Wiley and Sons; 1997.
2. Ahuja MK, Carley KN: *Network structure in virtual organizations, organization science, Vol. 10, No. 6, Special Issue: Communication Processes for Virtual Organizations, November–December*. 1999:741–757.
3. Mowshowitz A: **Virtual organization.** *Commun ACM* 1997, **40**(9):30–37.
4. Preuß S: *CH Cap, Overview of spontaneous networking-evolving concepts and technologies, in Rostocker Informatik-Berichte*, Volume 24. Rostock: Fachbereich Informatik der Universit; 2000:113–123.
5. Feeney LM, Ahlgren B, Westerlund A: **Spontaneous networking: an application-oriented approach to ad hoc networking.** *IEEE Commun Mag* 2001, **39**(6):176–181.
6. Latvakoski J, Pakkala D, Pääkkönen P: **A communication architecture for spontaneous systems.** *IEEE Wirel Commun* 2004, **11**(3):36–42.
7. Mani M, Nguyen A-M, Crespi N: **SCOPE: a prototype for spontaneous P2P social networking**. In *Proceedings of 8th IEEE International Conference on Pervasive Computing and Communications Workshops (PERCOM Workshops)*. 2010:220–225.
8. Legendre F, de Amorim MD, Fdida S: **Implicit merging of overlapping spontaneous networks**. In *Proceedings of Vehicular Technology Conference*, Volume 4. 2004:3050–3054.
9. Zarate Silva VH, De Cruz Salgado EI, Ramos Quintana F: **AWISPA: an awareness framework for collaborative spontaneous networks**. In *36th Annual Frontiers in Education Conference*. 2006:27–31.
10. Perkins CE, Bhagwat P: **Highly dynamic destination sequenced distance-vector routing (DSDV) for mobile computers**. In *Proceedings of the Conference on Communications Architectures, Protocols and Applications (SIGCOMM'94*. 1994:234–244.
11. Johnson DB, Maltz DA, Broch J: *DSR: The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks*. Boston, MA: Ad Hoc Networking (Addison-Wesley Longman Publishing; 2001.
12. Perkins C, Belding-Royer E, Das S: *Ad hoc on-demand distance vector (AODV) routing, RFC 3561*. 2003.

13. Park V, Corson MS: *IETF MANET Internet Draft "draft-ietf-MANET-tora-spe03.txt", November 2000*. 2012. http://tools.ietf.org/html/draft-ietf-manet-tora-spec-03 Accessed March.
14. Viana AC, De Amorim MD, Fdida S, de Rezende JF: **Self-organization in spontaneous networks: the approach of DHT-based routing protocols.** *Ad Hoc Networks* 2005, **3**(5):589–606.
15. Lacuesta R, Peñalver L: **IP addresses configuration in spontaneous networks**. In *Proceedings of the 9th WSEAS International Conference on Computers*. Athens, Greece: 2005:1–6.
16. Alvarez-Hamelin JI, Viana AC, de Amorim MDias: *Architectural considerations for a self-configuring routing scheme for spontaneous networks, Technical Report 1*. 2005.
17. Lacuesta R, Peñalver L: **Automatic configuration of ad-hoc networks: establishing unique IP link-local addresses**. In *Proceedings of the International Conference on Emerging Security Information, Systems and Technologies (SECURWARE'07)*. Valencia, Spain: 2007:157–162.
18. Foulks EF: **Social network therapies and society: an overview.** *Contemp Fam Therapy* 1985, **3**(4):316–320.
19. IBM: *A Smarter Planet*. 2012. http://www.ibm.com/smarterplanet.
20. Montenegro G, Kushalnagar N, Hui J, Culler D: *RFC 4944: Transmission of IPv6 Packets over IEEE 802.15.4 Networks*. 2007.
21. Alcaraz C, Najera P, Lopez J, Roman R: *Wireless Sensor Networks and the Internet of Things: Do We Need a Complete Integration? 1st International workshop on the security of The internet of Things (SecIoT)*. tokyo (Japan):; 2010. http://www.nics.uma.es/seciot10/files/pdf/alcaraz_seciot10_paper.pdf. Accessed January 2012 1er International Workshop on the Security of The Internet of Things (SecIoT 2010).
22. Ferscha A, Davies N, Schmidt A, Streitz N: **Pervasive Socio-Technical Fabric.** *Procedia Computer Science* 2011, **7**:88–91.
23. Hubaux JP, Buttyán L, Capkun S: *The quest for security in mobile ad-hoc networks, in Proceedings of the ACM Symposium on Mobile Ad-hoc Networking and Computing*. 2001:146–155.
24. Wang Y, Varadharajan V: **Interaction trust evaluation in decentralized environments, e-commerce and web technologies**. In *Proceedings of 5th International Conference on Electronic Commerce and Web Technologies, vol LNCS 3182*. Springer: 2004:144–153.
25. Jimin L, Junbao L, Aiguo A, Zhenpeng L: **Two-way trust evaluation based on feedback.** *in Conference on Logistics Systems and Intelligent Management* 2010, **3**:1910–1914.
26. Daskapan S, Nurtanti I, Van den Berg J: **Trust algorithms in P2P file sharing networks.** *Int J Internet Technol Secured Trans* 2010, **2(1–2):**174–200.
27. Maña A, Koshutanski H, Pérez EJ: **A trust negotiation based security framework for service provisioning in load-balancing clusters.** *Comput Secur* 2012, **31**(1):4–25.
28. Stajano F, Anderson R: **The resurrecting duckling security issues for ad-hoc wireless networks**. In *Security Protocols, 7th International Workshop Proceedings, Lecture notes in Computer Science, LNCS 1296*. 1999:172–194.
29. Balfanz D, Smetters DK, Stewart P, ChiWong H: *Talking to strangers: authentication in ad-hoc wireless networks, in Symposium on Network and Distributed Systems Security (NDSS'02)*. San Diego, CA: 2002.
30. Capkun S, Hubaux JP, Buttyán L: **Mobility helps security in ad-hoc networks**. In *Proceedings of the 4th ACM international symposium on Mobile ad hoc networking & computing*. MD, USA: Annapolis; 2003:46–56.
31. Metzger MJ: **Privacy, trust, and disclosure: exploring barriers to electronic commerce.** *J Comput-Mediat Commun* 2004, **9(4)**. http://jcmc.indiana.edu/vol9/issue4/metzger.html.

doi:10.1186/1687-1499-2012-203
Cite this article as: Lacuesta *et al.*: Internet of things: where to be is to trust. *EURASIP Journal on Wireless Communications and Networking* 2012 **2012**:203.