A Framework for User-Centered and Context-Aware Identity Management in Mobile Ad-hoc Networks (UCIM)

Abdullahi Arabo, Qi Shi, and Madjid Merabti
{a.arabo, M.Merabti, Q.Shi}@ljmu.ac.uk
School of Computing & Mathematical Sciences
Liverpool John Moores University, Byrom Street, Liverpool, L3 3AF, UK

ABSTRACT
The area of MANets (Mobile Ad-hoc Networks) is still in its infancy in the research community, but it plays a vital role surrounded by the growing trend of mobile technology for business as well as private and governmental uses. The concept of ubiquitous/pervasive computing is almost intrinsically tied to wireless communications. Emerging next-generation wireless networks enable innovative service access in every situation. Apart from many remote services, proximity services (context-awareness) will also be widely available. People currently rely on numerous forms of identities to access these services. The inconvenience of possessing and using these identities creates significant security vulnerability, especially from network and device point of view in MANet environments. The emergent notion of ubiquitous computing also makes it possible for mobile devices to communicate and provide services via networks connected in an ad-hoc manner. Digital identities are at the heart of many contemporary strategic innovations for crime prevention and detection, internal and external security, business models etc. This requires disclosing personal information and the applicability of contextual information as well as allowing users to be in control of their identities. In this paper we discuss the requirements for the development of an innovative, easy-to-use identity management mechanism within MANet environments. We convey various possibilities, challenges, and research questions evolving in these areas. The issues of context-awareness, making use of partial identities as a way of user identity protection, and providing a better way for node identification are addressed. We also examine the area of user-centricity for MANets together with its security issues and implications. We propose a framework for MANets that makes the flow of partial identities explicit, gives users control over such identities based on the respective situation and context, and creates a balance between convenience and privacy.

Keywords: user-centricity, contextual computing, Mobile Ad-hoc Networks, ubiquitous computing, identity management.

1 INTRODUCTION
The use of mobile handheld devices is expanding rapidly both within business and individual contexts. These devices are now essential tools for offering competitive business advantages in today’s growing world of ubiquitous computing. This has resulted in a proliferation of wireless technologies such as mobile ad-hoc networks (MANets), which offer attractive solutions to the services that need flexible setup as well as dynamic and low cost wireless connectivity. MANets can be defined as a platform or a set of nodes that can move freely and establish an ephemeral self-configuring wireless network.

With the emergence and development of wireless networks, the notion of “Ubiquitous Computing” coined by Mark Weiser [1] has received increasing attention. Tiny embedded computers with the abilities of computing and communication will be almost everywhere for the purposes of sensing, controlling and information displaying. One of the fundamental building blocks for such ubiquitous computing applications is MANets, and is increasingly used to support mobile and dynamic operations such as emergency services, disaster relief.
and military networks. Apart from many remote services, proximity services (context-awareness) will also be widely available. People currently rely on numerous forms of identities to access these services. The inconvenience of processing and using these identities creates significant security vulnerability, including the disclosure of personal information. This growing trend has raised serious concerns over Identity Management (IM) due to a dramatic increase in identity theft [2]. IM in this context is about managing relevant digital identities of a user and ensuring that users have fast, reliable, and secure access to distributed resources and services. The challenge is even bigger in service oriented network architecture, where partial identities are sprinkled across many services and users have no control for such identities.

In a nutshell, it be simply stated that ubiquitous computing has the capability of providing computational environments that facilitate the provision of information instantaneously through the use of “invisible interfaces”, consequently allowing unlimited spreading and sharing of information. If accomplish and developed properly, ubiquitous computing could offer an invaluable support for many aspects of our society and its institutions. However, neglecting the above mentioned privacy issues and aspects; there is a great likelihood that the end product will resemble an Orwellian nightmare[3].

To tackle the above problems, there is a need for a lightweight IM framework for MANets, which should be able to provide user-centricity, context-awareness and user friendliness. The first two abilities allow users to be in charge of adaptively controlling what identity information should be used, and how, when, where and to whom the information should be released, in relation to operational contexts. These are essential for IM to operate effectively in mobile, dynamic and even hostile MANet environments. The user friendliness ability is important for the wide adoption of the framework. Most users are not compassionate in knowing technical details involved in IM, particularly in complex MANet settings. It is thus crucial to build the framework in the way that separates users from complicated technical issues of IM in MANets and allows them to focus on its policy aspects. Additionally, due to the heterogeneity of devices used in MANets, the lightweight feature is necessary for enabling the framework to be operable in devices with limited resources such as low computing power and small memory. The lightweight feature is also applicable in terms of communication overhead, computation complexity, and storage overhead. Asymmetric cryptography is usually considered too expensive for MANets. Hence, symmetric cryptographic algorithms and one-way functions are commonly used to protect data integrity and confidentiality. User identity solutions and its hassle-free management play a vital role in the future ubiquitous computing. Current identity solutions can no longer cope with the increasing expectations of users in terms of usability and manageability.

The remainder of this paper is structured as follows. We discuss related work in section 2. Section 3 addresses the requirements of the proposed framework. Our framework is presented in section 4. Finally section 5 provides the summary and outlook of our work.

2 RELATED WORK

A MANet offers a temporary network without relying on any fixed network infrastructure, and communicates in a self-organizing manner. Moreover, MANets play curial roles in many application areas such as surveillance, marketing and military. While bringing huge benefits to these applications, they also raise serious privacy/security concerns. For example, some information could be used to track the whereabouts of users, monitor their behavior, collect information about them, and even incriminate some individuals based on the locations of their devices used in a crime as evidence against them.

Mobile users need to use identities for access to required services. An identity can be defined as something that can be used to identify a particular person or device. With regard to mobile devices, they have fixed identifiers, which essentially serve as mobile identities. This type of identity is also linked to other information on personal attributes including device locations, work addresses, telephone numbers, and user identities for managing the users’ mobile identities to enforce security and privacy protection. Such personal attributes are also called partial identities [4]. For the proposed research, we will consider both fixed and partial identities.

Each user of a mobile device is playing numerous roles in life to live. Hence, there is a need to organize the user identities in a more structured way, and such identities can be broadly categorized into three areas based on the roles the exercises in real life [5]. These are personal identity (PID), corporate identity (CID), and social identity (SID). PIDs can be used to identify a user in his/her very personal and commercial service interactions. CIDs and SIDs can be used in professional and social contexts, respectively, for interpersonal interactions. We can also say that individuals’ interests, preferences, or tastes are also part of their identities. These roles can be dealt with by users’ SIDs. Some of these identities are very sensitive in nature, so stricter authentication requirements have to be met. Some others require less secure infrastructure as they possess not so sensitive user information. Identity
information is closely associated with privacy issues.

Privacy as defined by Westin [6] refers to the claim of individuals, groups and institutions to determine for themselves, when, how and to what extent information about them is communicated to others. Hence, privacy is considered as an underpinning factor for the ultimate take up and success of MANets. Privacy can best be protected by enabling anonymous communication, which usually implies that a user remains un-linkable to a set of items of interest (e.g., communication partners and messages) from an attacker’s perspective.

One of the important principles of privacy is data minimization, which states that the collection and processing of personal data should be kept at minimal wherever possible. The broad aim of IM is to manage the resources of an organization (such as files, records, data, communication infrastructure and services) and to control and manage access to those resources in an efficient and accurate way (which in part usually involves a degree of automation). Consequently, IM is a technical and process-orientated concept. Evidently, IM has a chance to succeed only if it is clear from the beginning that users remain in control of their system and its interoperability with others with regard to their identity information. This indicates the need for user-centric IM for which some efforts have been made to develop solutions [7-10].

A notable approach is to consider IM as an integrated system of business processes, policies and technologies, which enables trusted organizations to facilitate users in access to critical online applications and resources while protecting confidential personal and business information from unauthorized users. There is also a growing consensus among legislators across the world that individual rights of privacy and the protection of personal data are equally applicable in the context of the Information Society as it is in the off-line world. To address this issue, a user-centric identity management framework is expected where users have complete control over the identity information transmission [11].

With the rapid development of MANets, IM is becoming an interesting and demanding research area. MANets could be formed at various geographical locations with nodes from different sources joining as well as leaving the networks dynamically in a self-governing style. This feature makes MANets much more exposed and susceptible to security attacks. Thus there is a pressing need for integrating context-awareness into IM. For instance, location information and users’ personal preferences for various operational settings can be used to dynamically and automatically configure mobile devices and user interfaces. Rule-based personalization algorithms can be too complex when handling user contexts and preferences; hence, there is a need for new mechanisms allowing dynamic adaptability of services. Semantic descriptions of user preferences and user relations with the combination of current developments in security and privacy issues can create more dynamic personalization. Such incorporation of context information into IM presents a complex research area and significant challenge to the research community.

Context-awareness also plays a crucial role in IM. Context is defined in [12] as “any information that can be used to characterize the situation of entities (i.e., whether a person, place or object) that are considered relevant to the interaction between a user and an application, including the user and the application themselves”. It is also worth pointing out that the research in accurately discovering contexts, efficiently disseminating contextual information, and making use of the available contexts is still at an early stage and has an important impact on the development of new/emerging applications in the area of ubiquitous computing [13]. In particular, context-awareness can facilitate users within a MANet environment to access and view services or available participants based on environmental context information in a dynamic and adaptive manner. For example, a user, who is within a city centre and looking for friends to socialize with, can make his/her social identity available within a nearby MANet and search for the friends within such an environment. This requires that services and related security settings be customizable in response to the contextual information provided.

2.1 Identity Management in MANets

MANets at first glance may not seem to be directly related to the issue of IM. IM normally gives the impression of a traditional client server structure, where users can establish a handshake with a server for authentication and other purposes. Peer to peer (p2p) networking also plays an interesting role in the context of IM as in this context users communicate directly with other users. However, MANets constitute technical infrastructures that could provide a base for both traditional client server and p2p applications. These technologies cause an enormous impact with implications for security such as packet forwarding and routing, network management etc., which are functions, carried out by all available nodes within the network. However, we are mainly concerned with the issues of context-awareness, user-centricity, privacy and user anonymity, as the information related to these issues can be used to track users’ whereabouts, monitor their behavior, collect information about them as well as incriminate individuals based on the location of the devices used in a crime as evidence against them. This can be achieved by building profiles of individuals from the partial identities used by them, which can be used to harm people’s privacy. As it stands at the moment,
such evidence will only point to the use of a device itself but may not prove that a particular individual is using the device unless – for example – some voice communication is involved.

In IMMANets (IM in MANets) we are not only concerned with fixed identifiers, but also with other personal attributes of a user, as we are more interested in identifying and providing security to the user of a device rather than the device itself. Partial identities on the other hand can be defined as a set of personal attributes of a user, where the user can have several partial identities, e.g. his/her work address and home telephone number [14]. Mohammad et al [5] categorized user identities as: personal identity (PID), corporate identity (CID), and social identity (SID).

Privacy refers to the claim of individuals, groups and institutions to determine for themselves, when, how and to what extent information about them is communicated to others. IM can be looked at in different contexts. One example is that it can refer to an integrated system of business processes, policies and technologies, which enables organizations to facilitate and control user access to critical online applications and resources while protecting confidential personal and business information from unauthorized users. In the case of mobile IM, location data may also include partial identities of the subject concerned.

Consequently, it can be seen that the issue of user privacy profiles is of crucial importance. Moreover, IM has only a chance to succeed if it is clear from the beginning that the user remains in control of the IM system. Interoperability of systems as such will not be accepted by users unless it is, by default, controlled by the users themselves.

This feature makes MANets much more exposed and susceptible to security attacks. Digital identity management becomes the heart of many contemporary strategic innovations, ranging from crime, internal and external security, business models etc. Thus there is a pressing need for cost-effective IM solutions in such environments. Hence, we can see that mobile IM is still in its infancy, where location information and users’ personal preferences for the configuration of mobile devices and user interfaces present a complex research area and significant challenge to the research community.

2.2 User-Centricity in MANets
User-centricity issues have been addressed by Eap et al. in which they propose an architecture based on a service-oriented framework called Personal IM that allows users to be in control of the management of their identities. User-centricity within the domain of Internet users is also addressed in fixed network settings. The requirements of MANets have not been addressed by Eap et al. Camenisch et al. have pointed out that user centricity is a significant concept in federated IM as it provides stronger user control and privacy [10]; they consider user-centricity abstractly and establish a compressive taxonomy encompassing user-control, architecture and usability aspects of user-centricity.

Bartolomeo et al. have also considered a shift from the technical-centric approach of current IM solutions to a user-centric one. They propose a user profile and design a distributed approach to manage user profile information and examine the possibilities for choice of a unique user identifier [15]. The issue of user-centricity has also been looked at from the point of view of its usage in Enterprise Directory Services to provide complete protection from the user’s perspective. It has been suggested that combining public key infrastructures, user-centric IM and Enterprise Directory Services would allow users to have control of the personal information stored within a directory as well as who is allowed to access the information [16]. Thus, a user may employ PKI to encrypt attributes, and then share decryption details with selected entities. User-centric IM has also been examined in [7, 17, 18].

One of the most essential aims of context-aware application is to deliver contextual resources efficiently and effectively [19]. In today’s real world, context-awareness is a key factor to the success of any ubiquitous application, which should enable conceptual data’s to be understood and communicated along with other entities in the system. Verkasalo proposed and developed a specialized algorithm that can be used in conjunction with handheld devices to acquire contextual information and classify them into home, office and on the move categories [20]. However, it is worth pointing out that by storing the information centrally, the problem of a single point of failure has not been addressed, and hence the network can be affected by compromising one of the nodes that stores the data.

2.3 Context-Awareness in MANets
Context is defined as “any information that can be used to characterize the situation of entities (i.e., a person, place or object) that are considered relevant to the interaction between a user and an application, including the user and the application themselves” [12].

Context-awareness is also of crucial importance in IM because users within MANet environments would be able to access and view services or available participants based on contextual information. For example, a user who is within a city centre and looking for friends to socialize with can make his social identities available within a MANet and search for friends within such an environment. Hence, services and security settings can be tailored based on the contextual information provided. Context-aware services are often viewed as a generalization of location-aware service,
subsequently many context-aware systems necessarily inherit the data management problems associated with any location-aware subsystems [21]. Context-awareness within the field of pervasive computing allows systems to adapt their operation based on the current contextual information without explicit user intervention and thus has the capability of increasing usability and effectiveness by taking contextual information into account. Putting this into the context of MANets, such networks might react specifically to the current location, time and other contextual attributes as well as adapting behavior according to the changing circumstances as context data may change rapidly. With regard to user-centricity and privacy, contextual information can play a crucial role in terms of allowing the policy maker to set privacy rules which depend on dynamic context data. For example, a policy can be set where access to specific information is either granted or restricted based on the location of the requesting user or device. Hence, context-awareness is one of the key elements for developing adaptive applications in ubiquitous environments and MANets in particular. Some of the research questions that need to be addressed in terms of context-awareness include amongst others, the following.

- What information should be sufficiently to describe a mobile user's identity so as to present the current mobile situation and context (e.g. location, personal information, general preferences set by users, temporal constrains etc.)?
- How should the data used to present a mobile user's identity be collected; i.e. which parties (e.g. network operators, law enforcement agencies, and profile providers, and/or service providers) should be involved in addition to the mobile user?
- What technical standards need be imposed so as to obtain access to these different components of mobile identities?
- Would it be necessary to introduce group identities such as work, friends, private etc. for easy privacy and policy management?
- What policies should be used in terms of negotiation of exchange of information of mobile identities?

A number of publications addressing context-awareness issues for the traditional Internet already exist and have been examined and tested within the research community. Examples include among others the work of Dinglaine et al. [22] on anonymous communication. Some of the basic principles of cultivating identities on the web and the importance of personal identities to oneself as well as others in order for them to recognize one’s contributions have also been examined [23]. Some location-centric isolation of misbehaving nodes in sensors networks has been proposed [24, 25]. This is of a data centeric nature and suitable for use in energy constrained networks. Camenisch et al. have pointed out that user centricity is a significant concept in federated IM as it provides stronger user control and privacy [10]; they consider user-centricity abstractly and establish a compressive taxonomy encompassing user-control, architecture and usability aspects of user-centricity. Some versions of centralized trust based security systems, which deal with the specific needs and challenges of MANets by combining decentralized security management and context-aware computing capable of establishing an appropriate trust level for various situations, have been proposed by Moloney et al. [26]. Hadjiantonis et al. [27] have also proposed a hybrid approach by employing a hierarchical and distributed organizational model for MANet management that has considered some aspects of context awareness and the capability of effectively managing a MANet. The issue of quality of context in pervasive context-aware systems for dealing with the complexity of context-specific operations such as acquisition, aggregation, reasoning and distribution has been addressed by Sheikh et al. [28], through the definition of five quality-of-context indicators for context-aware middleware. User-centric IM has also been examined in [7, 17, 18]. Recent publications have also looked at the issue of context awareness within the domain of publish-subscribe in mobile ad-hoc networks. Hence, the publish-subscribe paradigm has been extended with the ability to manage and exploit context information by using formal model based context-aware publish-subscribe implementations for MANets [29].

Verkasalo proposed an algorithm for hand-held devices to acquire contextual information and classified into home, office and on-the-move categories [20]. The algorithm classifies contextual data based on the usage of the devices involved. However, users can use their mobile devices for business purposes even when they are at home or on the move. We would like to propose a solution of profiling users and allowing the users to specify their own commitments at any point in time at home, on the move or in their respective offices while using their devices for different purposes rather than just taking the environment to decide what they are doing. Chen et al proposed a paper-based leaning support environment where mobile phones, traditional textbooks and web-based forums are integrated to promote students’ acquisition of knowledge. Students receive contextual messages from an online learning community based on their learning statuses [30].

3 REQUIREMENTS

In this section, an analysis of the requirements for our proposed framework is presented. The analysis
will be undertaken from three perspectives: anonymous communication, identity management, and usability requirements. The requirement analysis is expected to cater for the needs of end users and the key functionalities of the framework such as operation, mobility, security and personalization. The requirements can help answer two questions:

- What partial identities should be used in certain situations?
- Shall requested data be delivered in a specific situation to a particular requester, and what data be communicated if the delivery is permitted?

3.1 Requirements for Anonymous Communication

Anonymous communication is needed as a tool to protect a user’s privacy against one or more giving adversaries [4]. It is worth pointing out that most of the current anonymous communication mechanisms in use today are developed mainly for wired networks, whereby ad-hoc networks have other questions or issues to be answered differently. This includes the following:

- Can the existing mechanisms provide enough protection for ad-hoc users, meet the low energy requirements of devices involved, and offer good performance?
- Are the mechanisms dynamic enough to meet the required mobility of MANets?
- Can anonymity be possible for both large and small ad-hoc networks?
- Is it possible to provide total anonymity for ad-hoc networks without the use of a fixed infrastructure?

Hence, the following requirements for an anonymous communication mechanism might enable us to address the above issues in a more constructive manner:

- Scalability: Enables the mechanism to be dynamic enough to operate on different network topologies
- Security and reliability: Provide security against well-known protocol attacks, while maintaining the quality of communication
- Performance: Takes into account the issues of mobile devices’ limited resources such as low battery and processing capabilities
- Robustness to topology changes: Addresses the nature of dynamic topological changes in MANets to ensure the sustainability of security and performance
- Impedance of a fixed infrastructure: Makes the mechanism independent of any fixed infrastructure such as the Internet PKI
- Privacy and trust, Ensures the authenticity, confidentiality and unlinkability of information transmitted.

3.2 Requirements for Identity Management

Managing identity information plays a very curial role within our proposed framework. The following set of requirements is essential for guaranteeing users that their identities are well protected:

- Functionality: This includes handling and representing identities; having pseudonyms with specific properties and ability to recover real identities; enabling history management (i.e. storing and analysing communicated data or data flow); helping to identify which partial identity is used for what transactional context, when, where and how; allowing users to have control on their identities by choosing their required profile settings and preferences; and managing multiple identities of a user.
- Interoperability: One major characteristic of MANets is the variety of devices, e.g. PDAs, smart phones and laptops, which need to communicate with each others or that can be found within such a networking environment. Hence, the proposed framework should be able to handle and communicate with any of these devices effectively with little effort required from their users. The success of an IM system very much depends upon such ability to interoperate across a network of businesses, partners, and services regardless of the platforms, programming languages, or applications with which they are interacting.
- User-centric: It means the system should only reveal identity information about a user with his/her consent. Security is a main concern of this system. It should protect the user against deception, verify the identities of any parties who ask for the user information to ensure that it goes to the right place. In the user-centric approach, the user will decide and control the extent of his/her identity information to be transmitted. The system should disclose the least information needed for the user to gain requested services. By following these practices, the least possible damage can be ensured in the event of a breach. These are some of the requirements employed to
design a user-centric identity management system in The Laws of Identity [31].

3.3 Other Requirements

- User to be able to adaptively control information usage and disclosure
- Lightweight to be usable in energy and memory limited resource devices
- Customisable in response to available contextual information
- Location authentication - location authentication is of paramount importance with regard to security. Note that a device used in the network can be identified as being used at a certain location, but this does not imply that the device owner is using it, unless the owner authenticates himself/herself as the user.
- Location determination: This helps to identify users at certain locations, and to allow them to set the profiles that fit their commitments and possibly the environment.
- Security and privacy: To enhance security, users should be able to choose end-to-end data encryption. Unauthorised users should not be allowed to access, view, or modify identity information. With the growing awareness of privacy and the wish to protect it, users would be looking for more control over their privacy, in particular, what information is known about them and by whom. With an effective IM system, a user should be able to exert some control as to how much identity data they want to release (which may consist of approval for sending some particular identity attributes) as well as being able to retrieve data concerning the location of their identity data and who is able to currently access it. Users should also be able to stay anonymous while accessing some network services such as the network time protocol (NTP).

4 CONCEPT AND FRAMEWORK

A system scenario

Before going into the details of the proposed framework, it is worth making use of a scenario to illustrate potential privacy problems in the mobile ad-hoc domain that requires the use of contextual information to solve or minimize such problems.

Here, we will introduce an entity called “Ababa”. Ababa is out to get something to do during the weekend, so he tries to find some friends or people with a similar interest around the area while at the same time he wants to be able to control the information to be revealed to them. To achieve this, he joins a MANet using his new mobile phone. He is able to find a friend close by who sets his profile as available for social activities. Ababa uses the contextual information around the environment to locate his friend’s whereabouts, find suitable social activities around the area, and invite his friends to come over or play an online game while still being apart from each other. In this case, both users can make use of the contextual information, while being able to control the level of their identity information released to the ad-hoc networking environment.

We now propose our framework for User-centered and Context-aware Identity Management (UCIM) in MANets, which is depicted in Fig 1.

![UCIM Framework](image)

**Figure 1: UCIM Framework**

The framework consists of three main modules/components that perform different roles within the framework.

4.1 Contextual Information

The Context Provider: As the name indicates, it is responsible for acquiring contextual information from various contextual sensors or providers. We will represent contextual information as I. It is also responsible for processing contextual information into meaningful information that will be easily understood by non-technical users for its presentation within the user interface. Some of the contextual information that we have proposed to use include times, locations via the use of GPS signals while outdoors and Ultra-wide band (UWB) for indoors, and user profiles denoted by the symbol P. A user can set relevant information to present his/her current commitments and availability, e.g. at home or in the office, for social and other interactions, which is referred to as the context relation. This will be based on preset rules.

The Context Server: after the contextual
information has been acquired and processed. The information can be sent via the use of the pull approach to the context server. The main role of the context server is to store the information of the user and respond to the query of other users about the contextual information of the user/devices. It is also used to query other devices and store relevant information of the current devices for its own usage.

The Context Requestor module is responsible for invoking queries to both the Context Provider and the Context Server. It invokes queries to the Context Provider via the use of the push method, which is more of a real time response to the query only within the device itself. While the query via the Context Server is in the form of getting information about other devices within the MANet environment, the pull method is used.

One of the issues that need to be addressed in the contextual information is location authentication. Although a user’s location might show that his/her GPS location is in one place but he/she might be doing other things that are not related to the current location, e.g., the user’s GPS location shows that he/she is at home, but the user is busy with work related tasks, so the user sets his/her profile as office.

For the location authentication, we assume that a user can use his/her device for various purposes even in a giving location. The location information of the user can’t be modified by him/herself, but the user can specify its status (e.g., social, office, or work) to control the information that needs to be displayed.

Hence, the location authentication makes no guarantee about the user in control of the device or the actual status of the user at this point in time. However, such guarantees are provided by the identity of both the device and the profile setup of the user.

\[
UE \xrightarrow{\text{as the user environment or context provider}} I_0, I_1, I_n, \ldots I_n
\]

Where \( I_i = P_i \), activity, location (GPS), time etc

Where \( P_i \rightarrow \) status, activity, policies, information of other devices and users

\[
\text{ContextInfo} = \{ \text{name}, \text{value} \}
\]

**Figure 2: Contextual Relation**

Fig. 2 represents the UML contextual relationship model in which the following assumptions are made:

- **Context information**: consists of information like locations, user profiles, activities/statuses, etc
- **Context Relation**: describes the relationship between context information and context attributes including home, office, social, etc
- **Context Attributes**: list relevant information that needs to be stored to identify or represent contextual data.

### 4.2 Personal Identity Manager

The Personal Identity Manager consists of a set of user’s personal information, proposed information from the contextual information layers and the set of policies and rules required for the application. Each user is playing numerous roles in life to live. To organize the user identities in a more structured way, all user identities can be broadly categorized into three types based on the user’s roles/activities in real life [5]. These are personal identity (PID), corporate identity (CID), and social identity (SID). PIDs can be used to identify a user in their very personal and commercial service interactions. CIDs and SIDs can be used in professional and social interpersonal interactions respectively. Additionally, the user’s interests, preferences or tastes can be part of his/her identities, which may be dealt with by the user’s SIDs. Some of these identities are very sensitive in nature, and therefore stricter authentication requirements have to be met.

The Personal Information module contains a database of user details stored as an XML file. This structure is preferred to a normal conventional database because we are dealing with devices with limited resources.

The Contextual Data contains the processed data from the Contextual Information layer, where all relevant contextual information is processed and ready for usage by devices in a way that is understandable for users.

The Policy and Rules module deals with relevant security issues to protect users’ information from unauthorized access or disclosure. A user will be able to tick some boxes within a graphical user interface for the specification of the policies and
rules. Such rules will also be depending on the contextual information which must be evaluated if personal data is requested. The rules can further deal with issues of access control and data abstraction.

4.3 Privacy Manager

The Privacy Manager module consists of the profile info, privacy manager decision module and the profile zoning.

The profile info consists of attributes that users have selected to present their current profiles, e.g., if a user is at work, his/her profile attributes might comprise his/her office room number, extension number, calendar commitments, etc, as shown below:

Profileinfo = {officeDetails, commitments}

Fig 3 shows our early version of the implementation of the Privacy Manager module. Where users are allowed to use an interface to set

AccessControlRule (ACR) = {role, object, contextualconstraints}

DataAbstractionRule (DAR) = f [result(ACR), object, contextualconstraints]

Contextualconstraints=f {contextinfo, operation, referenceValue}

result(ACR) € {allowed, not allowed}

The privacy manager decision module makes use of the profile information and contextual data to determine to whom a user’s personal information can be released or made available within the given environment. This will classify the user’s personal information into two groups: allowed or not allowed for access by other users within the environment. This information is then passed on to the profile zone module.

The interaction between devices within MANet environments requires users to be able to select part of their identities (partial identities) that need to be visible to other users based on the contextual information. The identity information is defined as a set of attributes illustrated below:

Fig 3 shows our early version of the implementation of the Privacy Manager module. Where users are allowed to use an interface to set

//set of profile types
profileType = {Office, Social, Home, HealthCare}

ActionType = {triggerCommunication, makeAppointment, bookTable}

//relevant profile details
pIDProfile(office)=
{ Skills, commitments, officeNumber, room, calender }
pIDProfile(Home)=
{address, availability, phoneNumber }
pIDProfile(Social)=
{hobbies, birthday, phoneNumber }
pIDProfile(HealthCare)=
{insurance, bloodGroup, medications, history }

which attributes should be used to represent partial identities for Bank ID, Social ID, Insurance ID, Office ID and Home ID respectively. The implementation is based on the .Net Compact framework, programmed in C# and implemented within the Microsoft Visual Studio 2005 environment. It is simulated based on our in-house simulators for simulating some security vulnerabilities within a setting of system-of-systems scenarios.
Future work will be focused on completing the design and implementation of the Privacy Manager module. Our research has specified requirements. We are currently designing solutions for the Contextual Information and Identity Management in MANets with a balanced consideration of the requirements for identity management, and information in MANets environments, specified a set of options based on the context of a giving partial identity that the user requires.

In Fig 4, the user has access to different menu options based on the context of a giving partial identity that the user requires.

Figure 3: UCIM Interface

In Fig 4, the user has access to different menu options based on the context of a giving partial identity that the user requires.

Figure 4: Options Based on Context

5 Conclusion and Future Work

We have demonstrated security threats to identity information in MANets environments, specified a set of requirements for identity management, and proposed a framework for identity management in MANets with a balanced consideration of the specified requirements. We are currently designing the protocols for the Contextual Information and Personal Identity Manager modules, and also implementing the Privacy Manager module. Our future work will be focused on completing the design and implementation of the framework, and evaluating the efficacy of the framework implementation based on case studies.

REFERENCES


2


