

Context-Aware Group Communication in Mobile Ad-Hoc Networks

Dario Bottazzi, Antonio Corradi, and Rebecca Montanari

Dipartimento di Elettronica, Informatica e Sistemistica - University of Bologna
Viale Risorgimento, 2 - 40136 Bologna - ITALY
Phone: +39-051-2093001; Fax: +39-051-2093073
{dbottazzi, acorradi, rmontanari}@deis.unibo.it

Abstract. The widespread availability of both fixed and wireless network connectivity and the growing market of portable devices are enabling anytime and anywhere *impromptu* collaboration. The emergence of Mobile Ad-Hoc Networks (MANET) further opens up new possibilities for the provisioning of advanced collaborative services, such as civil protection, e-care, and troop car management. However, the design and the deployment of collaborative applications in MANET scenarios raises new group management challenges. In particular, MANET characteristics, e.g., unpredictable and frequent mobility of users/devices, intermittent device connectivity, continuous variations of network topology, make it impossible any a-priori knowledge about group members availability and ask for novel solutions to handle properly the communication about group members. The paper proposes a context-aware communication model to govern communication on the basis of the characteristics of the communicating parties, such as their location and their profiling information. The model provides communication patterns with different semantics to address both point-to-point and point-to-multipoint communication needs. The paper shows the implementation of the proposed model in the AGAPE framework for the design, deployment, and support of collaborative applications in MANET environments and presents the functioning of the AGAPE communication support in the context of a civil protection application scenario.

1 Introduction

The widespread availability of wireless network connectivity in the environments where users live and work, the increasing diffusion of portable devices, and the emergence of novel kinds of networks, such as Mobile Ad-Hoc Networks (MANET) create novel opportunities for applications that require *impromptu collaboration* between unknown partners sharing common interests.

However, the provisioning of collaborative services, such as emergency rescue, in environments with no fixed-network infrastructure and with constantly changing operating conditions raises new challenges and makes it necessary to re-think and to re-design traditional group management solutions [1]. Neither networks topology is pre-defined and fixed nor a-priori assumptions on the status and availability of group

members are possible. Group members appear and disappear in an unpredictable manner and frequently change their location and their access point of attachment to collaborative services; disconnection and network partitioning are common events. The scarce bandwidth provided by wireless network technologies makes the congestion become a normal and frequent condition. In this scenario, collaboration among users is inherently transient, it occurs among continuously varying and previously unknown partners.

Novel support solutions are required to address the different group management issues that arise in the provisioning of collaborative applications. Communication is a crucial aspect that recent research activities start to address along two main research directions: uncoupled versus coupled message-oriented communication models [2], [3]. We herein focus on message-oriented communication in collaborative applications deployed in MANET environments.

Traditional solutions cannot support group communication in the new computing scenario because it is impossible in MANET environments to rely on central naming solutions and to reach a global agreement on unique names among different members. The paper proposes to exploit visibility of context information, such as the physical position of users/devices, the preferences/characteristics of group members and the status of network operating conditions, to maintain and organize group members views and to enable effective group communication. In more details, we claim that context-awareness allows to identify a communicating party on the basis of its location and of its characteristics rather than simply depending on its name.

The paper presents the implementation of these concepts in the AGAPE (Allocation and Group Aware Pervasive Environment) middleware for the support of group membership management in MANET scenarios. In particular, the AGAPE communication solution provides several context-aware communication patterns, ranging from point-to-point to point-to-multipoint ones. An AGAPE group member can decide to communicate with one specific co-located member with a specific profile, or with a group member dynamically selected among a set of members with equivalent profiles or with multiple group members with desired characteristics. No predefined knowledge on group member names is necessary in AGAPE to enable communication.

The rest of the paper is organized as follows. Section 2 presents the new communication requirements in MANET environments, Section 3 describes the AGAPE framework, and Section 4 shows the applicability of the AGAPE communication solution in the context of a civil protection application scenario. Finally, concluding remarks follow.

2 Communication Requirements in MANET Environments

Collaboration in MANET environments calls for novel communication solutions ranging from point-to-point and point-to-multipoint ones. Few different approaches are starting to emerge that address communication for MANET scenarios [2], [3], [4]. Systems such as [2], [4] propose an uncoupled communication model that relies on shared tuple spaces. Tuple spaces provide shared dataspace to put and retrieve infor-

mation in an uncoupled way, by exploiting a pattern matching mechanism. That assumes the sender does know neither the receiver, nor when the information will be retrieved. Moreover, the receiver agent can retrieve information even with a partial knowledge of it. This is particularly useful in wide and dynamic environments where a complete and updated knowledge may be difficult or even impossible to achieve and where the sender and the receiver do not interact tightly. Systems such as [4] promote message-oriented communication styles. The sender identifies the destination of messages on the basis of their names and message delivery is restricted to destination entities. Collaborative applications that require spatially and temporal coupled communication can benefit from message-oriented communication models. This paper focuses on this kind of applications.

However, the development of collaborative applications based on message-oriented mechanisms require to address several other issues. Message recipients cannot be selected and addressed on the basis of their name attribute. Group member mobility makes it difficult to rely on a-priori knowledge about names, allocations and characteristics of possibly interoperating partners, thus making inappropriate traditional naming mechanisms. The exploitation of name for communicating with a group member requires complex location tracking mechanisms. But even if available, a group member name may be un-informative or insufficiently trustworthy in MANET environments where it is impossible to guarantee name identity uniqueness. Few recent solutions are starting to emerge that provide application designer with the possibility to deliver messages on the basis of recipient characteristics and not on recipient identity [5].

We claim that the development of MANET collaborative applications may benefit from context-aware message-oriented communication solutions: the selection of message recipients should depend on the applicable context and its dynamic evaluation. Different definitions of context have been recently proposed [6], [7]. In the following, we use context as the collection of any information useful to characterize the runtime situation of a communicating party during her service session, e.g., its location, its profile and its desired collaboration preferences. For instance, the location and the reciprocal position of the different interoperating parties is a key parameter to take into account into the design of communication solutions for collaborative applications.

In particular, MANET environments suggest to promote interoperation between co-located partners. In fact, several collaborative applications, such as civil protection, require tight collaboration between neighbors [8] and to enable communication among close members connected by short-length routing paths permits to save bandwidth and to improve system robustness. The impossibility to rely on stable network connections and to achieve acceptable error rates in message delivery through long-length routing paths makes it also technically difficult to enable collaboration between distant partners.

In addition to location attributes also profiles play a key role in controlling communication. There are cases that require to select message recipients on the basis of profile attributes. That is the case of a group member interested to know whether there is another member capable of providing specific functionality. The main advantage derives from the fact that a communicating group member becomes unavailable due to

unannounced disconnection/re-connection, a potentially new one with equivalent characteristics could continue communication.

To introduce the communication problem, let us consider a civil protection service that allows different users with different profiles, e.g., physicians, firefighters, engineers, and connected via lap-top computers to constitute a MANET network and to interoperate by exchanging SMS-like messages. The service should permit civil protection operators to interoperate with a specific co-located colleague, such as their boss, in order to solve a problem they have encountered during on-site aid operations. In addition, the service should allow fire fighters to alert one co-located physician to provide initial cares to an injured man. In this case, all co-located physicians are equivalent and messages should be delivered to a randomly chosen and close one regardless to her identity. Fire fighters should be capable also of communicating a warning message to a set of co-located colleagues.

This scenario exemplifies some of the possible and different communication patterns that can be needed among group members in MANET environments. We identify and propose three different communication patterns:

- **uni-cast** point-to-point communication. When one group member has to communicate, one and only one target member is selected. The chosen target is co-located and matches specific collaboration preferences. The pattern ensures that all messages are delivered to the designated entity as long as it is reachable. As a consequence, uni-cast permits to implement long lasting (possibly) stateful sessions of interoperation between two collaborating partners;
- **any-cast** point-point communication pattern. The pattern delivers messages toward a randomly chosen co-located entity that matches a specified profile. The pattern is suited for all situations where short lasting stateless collaboration activities are needed;
- **multi-cast** point-to-multipoint communication pattern. The pattern permits to deliver the same message to all the co-located entities matching the desired profile. Similarly to the any-cast pattern, multi-cast support short lasting stateless collaboration activities.

The choice of the proper communication strategy depends on a number of application specific factors, typically related to the execution context and to the characteristics of the service.

All aforementioned communication patterns require appropriate support solutions to properly manage binding between communication parties and to re-qualify obtained bindings at run-time depending on the dynamic execution conditions. There are two main binding requirements. The uni-cast pattern requires the possibility to obtain the reference to the needed co-located member and to maintain it until it is reachable. On the contrary, in the case of any-cast and multi-cast patterns the obtained references do not have to be maintained during communication, but change dynamically to refer to different group members at any message exchange. The only constraint is that the new binding should refer to a new group member in the same locality with equivalent properties.

3 The AGAPE Framework

AGAPE supports the rapid design, development and deployment of context-aware interoperation among users operating via mobile terminals in MANET environments. Collaboration in AGAPE is based on the metaphor of group where the interoperation is restricted to the entities that are member of the same group. Each group is characterized by a group unique identifier (GID) and by a profile that specifies interests, preferences, activities and goals that should be commonly agreed by all members of its. The set of members that compose a group cannot be determined a-priori. On the one hand, new members may join/leave the group at run-time depending on application-specific requirements, and, on the other hand, user terminal mobility may cause unannounced group partitions/merges.

The notion of locality is central in AGAPE to support group management. A locality is defined as the set of AGAPE entities that are placed at a reciprocal distance lower than a determined threshold value. This value is expressed in network hops and determines the maximum dimension of a location. In particular, the entities in one locality may belong to the same or to different logical groups. An AGAPE group may be partitioned into disjoint sub-sets, called clusters, that assemble co-located group members. Note that several clusters belonging to different groups may co-exist into one locality.

AGAPE identifies two different kinds of group member entities in each cluster: cluster head (CH) entities and managed entities (ME). CH is a dynamically designated management entity which is in charge of performing group management activities within the scope of the associated cluster. For example, it is in charge of admitting/rejecting join requests and of providing managed entity a perception of the group, i.e. a view, that is limited to the scope of the actual cluster. ME exploits CH group management functionality to interoperate with co-located ME. Each group member, both CH and ME, is characterized by a personal identifier (PID) which is assumed to be unique within the group [11].

3.1 The AGAPE Middleware

The AGAPE middleware provides the needed services to support group management operations in MANET environments. We herein focus on the description of the main distinctive AGAPE services to support binding and communication. Figure 1 shows the most important services grouped in two logical layers. The group layers propagates the visibility of the group members within a cluster up to the application level and provides the services necessary to enable the formation and the maintenance of groups. The communication layers provides collaborative applications with asynchronous, unreliable message-oriented communication primitives that implement uni-cast, any-cast, and multi-cast communication patterns.

The **Proximity Service** (PS) provides discovery facilities and permits AGAPE members—both CHs and MEs—to advertise their on-line availability. At regular times

member entities broadcast a beacon to all the direct neighbours. The beacon includes both GID and PID of the sender along with the role played into the cluster (either CH or ME). In addition, a Time to Live (TTL) field that expresses the number of hops the message is to be propagated is included. Upon reception, the receiver decrements the beacon's TTL and (if non-zero) retransmits the message to all its direct neighbours with a probability $p(n)$ which decreases if the number of entities located in proximity increases. This approach permits to avoid broad-cast storming. Only group members advertise their availability but, according the TTL field, each AGAPE entity—both members and not members—are supposed to retransmit beacons. This service does not relies on existing discovery solutions, such as Jini and UPnP, because their implementation does not address well MANET settings.

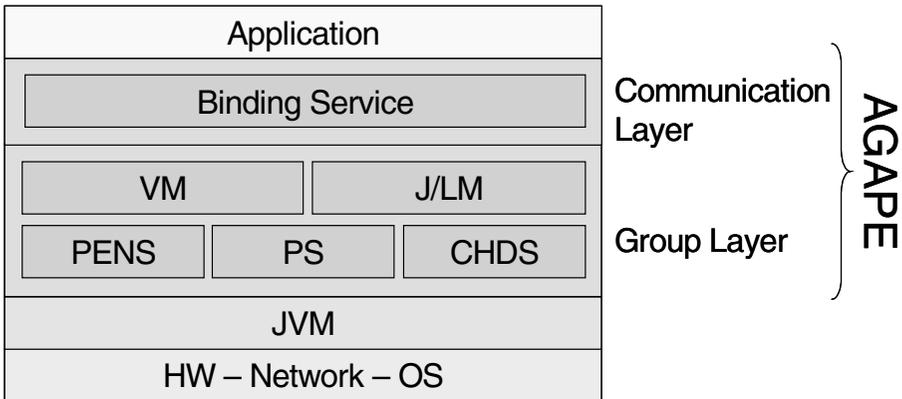


Fig. 1. The AGAPE architecture.

The **Proximity Enabled Naming System** (PENS) is in charge of randomly generating GIDs and PIDs. In particular, similarly to the naming solutions proposed for P2P environments [11], only statistical identifier uniqueness is provided. In addition, PENS maintains an updated table of co-located AGAPE entities that possibly belong to different groups and group clusters. The service senses incoming packets broadcasted by the proximity service and, according to the received information, builds a table which associates members GID/PID and role (CH/ME) with their IP address. Whenever packets from a new member entity are detected, a new entry into the table is generated. Analogously, if the reception of packets from a given member included into the table exceed a determined delay, the associated entity is removed from the table. Any change in table information is represented in terms of an event and notified to interested entities.

The **View Manager** (VM) service is in charge of creating, disseminating group views to AGAPE group members. Each group member receives a view—called Context View—that contains the list of only group member located within the scope of a cluster. In particular, each Context View entry associates each member reference with user/device profile information—such as GID, PID, user interests, age—that are necessary during the process of message recipient selection. When group members con-

nect or disconnect from the network, AGAPE reports the view changes to all interested group members into the cluster. In addition, VM customizes the context views delivered to group members on the basis of their collaboration preferences. Delivered Context Views contain only the locally available group members that match the collaboration preferences expressed by a group member at its group joining phase.

The **Join/Leave Manager** (J/LM) service allows not member entities to join the group and to member entities to leave it. By exploiting the PENS, locally available groups can be discovered. In particular, the CH entities are discovered and their visibility propagated at the application level. The joining phase consists in first contacting all discovered CHs and ask for their group profile. If a group of interest is retrieved a join request is sent to the CH in charge of group management. The join request message includes candidate member profile along with its profile describing its characteristics and the desired collaboration preferences. According to the installed management policies CH decides whether to accept or to reject the join request. In the case of acceptance an acknowledge message is replied that includes the GID/PID generated by PENS for the new member. Finally, the Join-Learn Manager coordinates with the View Manager in order to distribute to the group member the Context View related to the cluster of interest. When a member leaves a group the Join-Learn Manager coordinates with PENS to delete the GID/PID of the member willing to leave and with the View Manager to update the Context View.

The **Cluster Head Designation Service** (CHDS) is in charge of electing a new cluster head. A variation of the election protocol proposed for MANET in [9] is exploited to designate the new CH entity. The election is triggered either by the unavailability of the Cluster Head or by its inability to continue to carry on its management duties due to events, such as battery degradation or the decreasing of free memory.

The **Binding Service** (BS) supports message-oriented communication by managing on behalf of group members the bindings with their communicating parties. BS provides different binding management strategies depending on the communication patterns exploited. In particular, when a group member wants to establish a communication, it contacts BS, provides it with a Searching Profile (SP) specifying its collaboration preferences and specifies the desired communication pattern. BS exploits the SP to filter the content of the locally available Context View in order to retrieve the list of all co-located group members that match specified profiles along with their addresses (target members set – TMS). Then, BS builds a record including various fields: the GID/PID of the requesting group member, the SP, the TMS and the desired communication pattern. Each record is stored into the Binding Table directly managed by BS. Finally, BS returns to the requesting group member an handler to the record in the Binding Table. If the uni-cast communication pattern is selected, BS binds the requesting group member with the first group member in the TMS as long as it is reachable. In the case of any-cast and multi-cast communication patterns, BS binds at each message exchange the requesting group member with the first available group member in the TMS.

In addition, BS constantly keeps the TMS in the Binding Table records updated through the coordination with the View Manager service. In particular, if a relevant change in the Context View occurs, the TMS field of the Binding Table records is updated accordingly. This allows to dynamically re-qualify bindings when needed.

4 Case Study

To illustrate the functioning of the AGAPE communication support let us consider a simplified civil protection application scenario that allows impromptu interoperation between co-located operators in case of major disaster. In this scenario, the impossibility to make any assumption about the availability of network connectivity through Tetra, GPRS and UMTS channels suggests to exploit MANET infrastructure support. Our civil protection application prototype enables user to interoperate by exchanging SMS-like messages without the need for connectivity to the Internet, in a decentralized fashion, by exploiting the full-visibility of only locally available group members.

In our prototype, a Mobile Ad-Hoc network is dynamically constituted by exploiting 802.11b-enabled laptops provided to the different civil protection operators. The operating system we installed on lap-tops is Linux; to implement the MANET infrastructure we have configured lap-tops to include the AODV [10] routing protocol. Moreover, due to the lack of standard addressing schema for MANETs, we have statically configured device IP addresses. These deployment setting choices do not undermine the generality of the results. The AGAPE infrastructure does not depend on the availability of a specific routing protocol or addressing schema.

All AGAPE services are installed on each device and implemented on top of J2SE 1.4. As a consequence each user device may become on its turn either CH or ME.

The application aggregates together in one single group civil protection operators operating within the same area. Different users have different roles and competences and, as a consequence, they are characterized by different profiles. These profiles along with their used access terminal characteristics have been modeled as CC/PP profiles. For description simplicity, and without lack of generality, let us suppose that the profile includes only operator's name and skills (e.g. engineer, physician, and so on).

Let us show how AGAPE works by considering the case of one civil protection operator that promote the dynamic formation of the civil protection group at execution time. To this aim, the application client module of the civil operator allows him to specify the group profile—in our example “Civil Protection”—along with the user own profile—for example “Tom, Firefighter”. Then, the operator's lap-top exploits the locally installed PENS to generate GID/PID and the View Manager service to initialize Context Views. The operator's laptop advertises by means of the Proximity Service its on-line availability by sending beacon messages. All lap-tops into the locality can therefore benefit from the visibility of the novel Cluster Head. In particular, not-member entities can query the discovered CH to the purpose of obtaining the group profile. In our example, the different entities recognize that the CH is associated with the civil protection application and request it to join the associated group by sending it a “Request to Join” message. The message includes member profile along with the preferences about desired interoperating partners. For example, a fire fighter may require to interoperate only with fire fighters and physicians. Then, if the CH admits the new member, the Group ID along with the Personal ID that identifies the entity within the group, are delivered to the new member. In addition, the CH updates the Context Views and installs them on the new member. Note that the installed Context View reflect the preferences made at the join request. In the described example

the Context View delivered to the fire fighter device will include only fire fighters and physician members.

Let us now consider how AGAPE takes care of communication in the case an any-cast communication pattern is selected, for instance when a fire fighter wants to alert one physician—regardless to her identity—to asks for her intervention. To communicate the alert message the application that runs over the fire fighter’s lap-top must obtain a handler to the Binding Table. To this aim, the application specifies the required communication pattern along with the Searching Profile. In particular, the SP states that the desired members for collaboration are physicians. The Binding Service on fire fighter’s computer filters the delivered Context View to identify all members with a profile that matches the provided SP, i.e. all physicians, located into the cluster. Then, the Binding Service creates a new entry into the binding table. This entry must be referred to dynamically determine the recipient of messages to be sent. Note that the Binding Service updates the entry into the table according to the information it periodically gathers from the View Manager, thus dynamically re-qualifying the bindings.

5 Conclusions and Ongoing Work

The design, development and deployment of group membership and communication systems in MANET environments raise challenging issues. As a consequence it is necessary to re-think and re-design traditional group management solutions. AGAPE intends to give a contribution to the research area of middlewares to support group-aware applications in MANET environments.

AGAPE supports collaboration through the metaphor of group. Only group members entities are enabled to collaborate together. As a key feature, AGAPE implement different communication patterns that exploit the visibility of the location of group members along with their profile as a first-class concept to select and refer to desired communicating entities.

For the sake of description simplicity of AGAPE functioning, we have presented a simple civil protection application prototype built on top of AGAPE, but we are experimenting the AGAPE middleware in a wide variety of scenarios. First experiences in the use of AGAPE have shown that our middleware can simplify the design and implementation of collaborative services. These results are stimulating further research along different guidelines to improve the current prototype and to develop more complex services on top of it. We are currently working on evaluating alternative group member management models. In particular, we are investigating the possibility to rely on fully decentralised management solutions with no local central point of management, i.e., without a CH in each locality. We are also testing different algorithms for optimizing bandwidth usage of the probabilistic flooding protocol implemented by the Proximity Service. In addition, we are investigating the security concerns that group management arises by starting to integrate initial security support services in AGAPE.

Acknowledgements. This investigation is supported by MIUR within the framework of the FIRB Project "WEB-MINDS" and by CNR within the framework of the Strategic Project "IS-MANET".

References

1. D.Powell (ed.) "Group Communication", Special Issue on Group Communications, Communications of the ACM, ACM Press, Vol. 49, No.4, April, 1996.
2. G.Picco, et. al., "Lime: Linda meets Mobility", Proc. 21st Int. Conf. on Software Engineering ICSE1999, CA, May 1999.
3. L. Capra, et. al., "XMIDDLE: A Data-Sharing Middleware for Mobile Computing", Personal and Wireless Communications Journal, Kluwer, Vol. 21, No.1, April 2002.
4. G. Kortuem, et. al., "When Peer-to-Peer comes Face-to-Face: Collaborative Peer-to-Peer Computing in Mobile Ad-hoc Networks", Proc. International Conference on Peer-to-Peer Computing (P2P2001), Sweden, Aug 2001.
5. M.A.Munoz, et. al., "Context-Aware Mobile Communication in Hospitals", Special Issue on Handheld Computing, IEEE Press, Vol. 36, No.9, September, 2003.
6. A.K. Dey, et. al., "Towards a Better Understanding of Context and Context-Awareness", Proc. of Conference on Human Factors in Computing Systems CHI2000, Netherlands, April 2000.
7. T. Rodden, et. al., "Exploiting Context in HCI Design for Mobile Systems", Proc. of Workshop on Human Computer Interaction with Mobile Devices, Scotland, May 1998.
8. G. Kortuem, et. al., "Wearable Communities: Building Social Networks with Wearable Computers", IEEE Pervasive Computing Magazine, Special Issue on Wearable Computing Technologies & Applications, October-December 2002.
9. N. Malpani, et. al., "Leader Election Algorithms for Mobile Ad Hoc Networks", Proc. 4th International Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications, 2000.
10. C.E. Perkins, et. al., "Ad hoc On-Demand Distance Vector Routing." Proc. of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, LA, February 1999.
11. A. Rowstron, et. al, "Pastry: Scalable, distributed object location and routing for large-scale peer-to-peer systems". Proc. IFIP/ACM International Conference on Distributed Systems Platforms (Middleware), Germany, November, 2001.