2017 IEEE 37th International Conference on Distributed Computing Systems Workshops

Policies Guiding Cohesive Interactions among Internet of Things with Communication Clouds and Social Networks

Henry Hexmoor
Computer Science Department
Southern Illinois University
Carbondale, IL, 62901, USA
hexmoor@cs.siu.edu

Bidyut Gupta
Computer Science Department
Southern Illinois University
Carbondale, IL, 62901, USA
Bidyut@cs.siu.edu

***Abstract*— Cohesive interaction among Internet of thing nodes will benefit from formation of ad hoc communication network clouds for rapid exchange of information that is pertinent for their successful interaction. Long enduring interactions among such nodes will benefit from ad hoc socially linked networks for collaboration on shared objectives. We present guidelines for forming and using these constructs and domain-neutral policies that constrain them to specific applications.**

Keywords- internet of things, social network, cloud network, collaboration

I. INTRODUCTION

We inhabit a world that is increasingly populated with networked Internet of physical things (IoT) as well as dis-embodied internet of virtual agents (IoA) [1][2] [5][6][12]. We need high-level methods to control and express our desired behaviors over them at various scopes, both temporally and spatially. Our current focus is to facilitate interactions. Subsequently, high-level control issues will be addressed via codified principles captured in control rules and policies that remain beyond our scope. For instance, consider an eldercare house where mobility devices (e.g., wheel chairs and medicine dispensers) must move rather slowly in the bedroom whereas meal delivery system must be punctual and meticulously mindful of the resident's medical prescriptions. Policies can provide means of globally apportioning communication resources and arbitrating among objectives shared among IoT and IoA nodes. Recently, we have conceived of the use of P2P logical overlays and social networking principles for environments that allow IoT nodes to interact and engage in social interactions when they wish to share in information and collaborative tasks [6]. In order to expedite communication, nodes will initiate and join ad hoc overlay networks such as a cloud network [11]. For instance, vehicular networking groups have devised ad hoc cloud networks combined with principles of content-based networking where events and information is as well as storage and processing are resources that are shared as the vehicular needs arise [9]. Such communication networks are spontaneous and exist for fixed and intended time durations. Often, interactions among participants of these volatile networks will transcend many impromptu communication networks. Continued interactions among any pair of nodes are *links* that will create familiarity and rapport between nodes for more cohesive future interactions. There might be a persistent set I= $\{I_1, I_2, \ldots, I_n\}$ of information resources shared between a pair of nodes (e.g., an event such as a traffic signal or a destination that is shared between vehicles or the health status of a resident) that is an intangible information oriented resource set. Such as set is derived from examining patterns of interactions with the objective to improve communication efficiencies. The process of constructing set I is easily automated by allowing each node to nominate an entry in the set as long as a second affected node approves the nomination of the entry. Most often, common, scarce, or unique resources shared among nodes can be impetus for sharing information. Separately, there might be a persistent set O = $\{O_1, O_2, \ldots, O_n\}$ of objectives between a pair of nodes (e.g., congestion avoidance, road safety among vehicles, or patient hydration level). Unlike set I, set O must be strictly encoded when an IoT and IoA nodes are designed. Detecting shared objectives among odes is a nontrivial problem.

In the next subsection, we will articulate a generic set of steps that account for formation of spontaneous social networks between nodes starting with pairwise social links. This is followed by a set of generic steps that prescribe spontaneously formed cloud networks. The remainder of the introductory section outlines high-level guidelines for when social networks and ad hoc clouds can be formed. Section 2 generically articulates rules and policies over these situated structures. Section 3 offers a brief review of related work. Concluding remarks are given in section 4.

A. Steps Governing Social Networks

Definition-- initiate a *social link* (i, j, I, O): An ad hoc social link between nodes i and j are initiated (with a unique ID) when three conditions are met: (a) there is one or more shared objectives in O between the pair of nodes, (b) i and j have one or more shared information resource in I (e.g., safety status in a situation) between them, and (c) there is no prior duplicate link with between the pair given I and O.

This step of establishing social link creates a new dyadic ad hoc social link with a unique ID and such a social link is limited to the specific pair of nodes. Three or more nodes (i.e., with two or more links) may form a *social network* for greater collaboration stated in the social network initiation

1545-0678/17 $31.00 © 2017 IEEE
DOI 10.1109/ICDCSW.2017.24

step but before we go further we must acknowledge that social links are volatile and may terminate, that is stated next.

Definition—Abandon social link (i, j, I, O): The social link between i and j is abandoned and becomes defunct forever iff one or both of the following conditions are met: (a) the specific, original member of O is no longer of interest due to completion or mutual lack of interest in them, or (b) the shared information resource in I is no longer accessible.

An abandoned link is obsolete and is no longer used to facilitate collaboration between the pair of nodes. Next, we establish a kind of social network formation among nodes on disparate pairs of social links in set of dyadic links L = {L_1, L_2, … L_k}. Such a situated formed social network supplants the group's disparate links.

Definition – Group Initiate SN (I, O, L, T): Two or more social links that are members of social link set L that collectively share resources in I and objective in O may become a uniquely social network (with a designated ID) for time duration T when all nodes agree to be beneficent toward one another for achieving O and sharing resource in I. The idea of becoming a social network is reminiscent of research efforts in AI for defining conditions for team formation and maintenance. However, social networks have the added requirements that members possess strong allegiance to the group and helpfulness (beneficence) toward others in the group.

All links involved prior to formation of a social network are usurped with the links used in the newly formed social network. Social network initiation jointly belongs to all nodes and all nodes have equal right over the resulting network. Nodes may join or leave the network stated in later steps. An alternative step for an ad hoc social network formation is when an intrepid node decides to discover a mutual objective that can be shared with a group of its peers stated next.

Definition – Individual Initiate SN (i, N, o, T): A node i who is a member of peer nodes N, will multicast a mutual objective inquiry about an objective o to all nodes in N, will receive and collect mutual objective agreement from a set S that is a subset of N. Node i then forms a social network with S using a unique social network (with a unique ID) with time duration T. The social network that is originated by single node bears the advantage of a single objective put forth by one agent but it is somewhat subject to the domination of interests of that agent. Despite this, nodes may join and leave (in the following definitions) with both type of social network and contribute equally to its continued use or its demise.

Definition-- Join SN (ID, I, O): A node will join the specific IDed ad hoc social network in one of two conditions: (a) the node has acquired an existing social link with a member of the social network, or (b) the node agrees to beneficence toward access to a specific resource in I and allegiance to achieving the shared objective O. Once joined. the link with the external member will be absorbed into the social network and will cease independent existence.

Definition-- Leave SN (ID, I, O): A node will unilaterally leave the specific IDed social network in one of three conditions: (a) it has lost all its existing social links in the SN, (b) it has lost its beneficence to others, or (c) it has relinquished its allegiance to achieving the shared objective O. The last condition arises from a node joining a competing social network. Once a social network is formed, it must be used to maintain it or it must be dissolved. A SN will work as a benevolent cohesive team in the context of R and O. Usage of this structure is stated next.

Definition—Use SN (ID, I, O): A node that is a member of a SN with a given ID may engage in interaction in one of two ways: (a) the node accesses a shared resource in I, or (b) the node will jointly work on an objective in O with one or more SN members. Either situation will increment the usage frequency of SN. A SN is released if the originating objective is no longer active, resources are inaccessible, links are abandoned, or it has not been used for a long duration. This is articulated next.

Definition-- Release SN (ID, I, O, L, T): A social network with a given ID in the context of R and O can be abandoned in one or more of four conditions are met: (a) O is no longer of interest due to completion or lack of interest, or (b) I is no longer available, (c) all links L are abandoned, (d) no member has used it in a predefined time duration T.

In order to facilitate efficient peer-to-peer communication, among nodes that may share information resources, ad hoc communication clouds are proposed [10] [11]. At times, using an ad hoc cloud is seen as information and sensing as a service. We state the basic guideline for cloud formation next shrouded in information resource discovery. Let C be a set of nodes (e.g., IoT nodes in an automated nursing home) and I be an information resource set (e.g. health status of a resident).

B. Steps Governing Ad Hoc Communication Clouds

Definition—Initiate cloud (C, I, T): A member i of C will multicast a *resource request* to members of C for data related to a specific member of I. A subset S of C will send resource *response message* to i that each has data that is relevant to I. i then forms an ad hoc cloud network with members of S and adds itself to S as the cloud master with a generated unique cloud ID. By default, this ad hoc cloud will expire after period T prescribed by the cloud master as a function of expiration period for I. A node may initiate multiple clouds each over a pair of C and I. To avoid duplication, for a pair of T, and I cloud request for only one member of C will be granted. Once a CIT cloud is formed, other nodes in C beyond S may join a cloud network stated next.

Definition—Join cloud (ID, C, I, S, T): A member j of C may join cloud ID to access I if the following two conditions are met: (a) it is not already a member of S, (b) if the cloud master in S does not see a conflict for j accessing resource I. The main purpose of a cloud is usage is stated next.

Definition— Use cloud (ID, C, I, S, T): Once a cloud ID with members S and information resource I is established; periodically, the cloud master will issue data update request from members of S and collects them to upkeep the information resource I.
Just as joining, some members may wish to leave the cloud for their own reasons.

Definition—Leave cloud (ID, C, I, S, T): A member i of S may leave cloud ID for any reason without permission from anyone. S is updated to delete i from S.

When resource I becomes obsolete or all members have departed, the corresponding cloud may be abandoned, given next.

Definition— Abandon cloud (ID, C, I, S, T): Cloud ID is abandoned if (a) S is empty, (b) I is obsolete according to cloud master, or (c) cloud life time has reached its default life span T unless the cloud master refreshes or extends the cloud life. In a given environment, a node may simultaneously and independently initiate and participate in multiple cloud networks as well as multiple social networks.

II. RULES AND POLICIES

A common class of rules are found in computer networking that pertain to routing from sources to destinations and a variety of access control and paths selection we'll dub *provenance rules*. These rules have the general structure of <cloudID, source, destination, info-type, action>. Possible general actions include forward, drop, update-refresh-rate, and count. Since an information resource forms the genesis of a cloud network and plays a central role in a social network, corresponding provenance rules are useful for setting up their scope among interested parties as well as their producers and consumers.

An example of a provenance rule is (cloud3, lead-vehicle, follower-vehicle, congestion-report, update: 0.05), which specifies an update rate for congestion from the lead vehicles to followers in cloud 3.

At any given time, there will be as many provenance rules as the cardinality of set I. A policy is a system of customizing combining rules for a specific context or application [16]. Although it is possible to suggest policies to prioritize the provenance rules and to arbitrate conflict among them, this strategy is cumbersome, rife with complexity, and possibly contain many exceptions. An example of a policy to ordering rule precedence among four rules is (r4, r3, r2, default: r1) where rue 4 subsumes rule r3, and in turn r3 subsumes r2. When neither of these policies are in effect, r1 is the default rule.

Following principles of software defined networks, specific network applications will direct network management in particular ways. We envision, high-level policies can be designed to encapsulate each application. More specifically, policies will manage ad hoc clouds and social networks. In the eldercare example, policies for network management for first responders could suppress the routine traffic with emergency traffic. Similarly, in vehicular settings, policies for an accident application or a weather incident would expedite that information broadly in favor of routine driving network traffic.

Cloud networks are rather spontaneously formed among strangers around a volatile information resource and often there is no opportunities for social connectivity and social networking as subordinate structures. On the contrary, a long enduring social network may contain cloud networks within it as its proper subsets, which indicates an environment that is rather stable shown in Figure 1. Three clouds connect pairs of vehicles respectively over information resources I_1, I_2, and I_3. Whereas the social network is made up of three pairs of social links (v1,v3), (v2, v5), (v4, v6). Presence of a cloud network inside a social network will improve social links via ease of communication. Presence of a superset social network is a predictor of cloud network formation since sharing objectives will make it necessary to share information resources.

Given the relative stability of social networks, objectives can often be traced to organizational charters among dwelling nodes. As such, governing provenance rules belong to those organizations. Policies will also be closely tied to the organization.

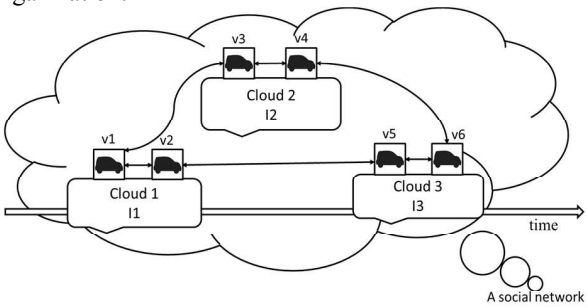

Figure 1. Social networks may contain cloud networks

Returning to the eldercare example, mobility devices, medical nodes, and other support nodes will often be members of the eldercare facility and use the facility operating provenance rules. Similarly, policies would be contained in the facility and organization of eldercare.

A policy for an ad hoc cloud can be very intricate and specify conditions and contexts of its application. By and large, there are general attributes that characterize a communication policy that is applicable for ad hoc

communication clouds. Firstly, a policy needs to identify an applicable time window (called *lifespan*). In our ad hoc network guidelines, we specified an expiration period time period T that serves this purpose. This could be tied to the actual system timeline. A second attribute (called *structure*) specify the scope of affected nodes. The actual policy permissions or restrictions form the third attribute (called *rule order*). The fourth attribute identifies a master node who may introduce exceptions to the policy in an ad hoc network (called *master*). Together, an abstract ad hoc cloud policy is <lifespan, structure, rule order, master>.

A policy for an ad hoc social network may constrain myriad facets of social interconnectedness among its members. By analogy, a social network is a construct that behaves as an organization and at times like a biological family.

III. RELATED WORK

Things in physical proximity form social links creating social networks. Minimally, things provide profiles that include goods and services relevant to other things [3][4][6][5][7][8][9][15]. Hence, we will refer to them as Social networks for IoT (SIoTN). Although there are attempts in introducing SIOTN, there is yet little systematic research for integrating them with communication networks.

Communication networks are producing ever more tunable network functionalities using overlay networks and software defined networking (SDN) [13][14]. Figure 2 shows the basic SDN components at a high level. Traditional packet forwarding and routing on the data plane is on the south side of SDN control plane directed by the core services and instructions from the SDN controller similar to an operating system. Network applications determine the behavioral modalities of network functions shown on the north side of SDN controller.

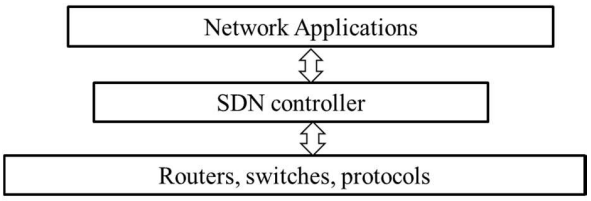

Figure 2. High level components of Software define Networking (SDN)

Ad hoc cloud networking is another flexible communication strategy that has been suggested for vehicular ad hoc networks [15] as well as for the IoT [10]. Clearly, impromptu nature of ad hoc overlay networking as an amalgam of software defined and cloud networking are the dominant communication trend that underlay our approach.

Our suggested logical ad hoc networks are only feasible as the need arises to activate subnetworks of traditional communication network layers on which the nodes dwell upon. Figure 3 depicts the progression of logical versus traditional communication networks. When Alice and Bob consider establishing a social link or a private ad hoc cloud, the corresponding logical level triggers a P2P peer discovery, authentication, and instantiation within the P2P overlay network that had been constructed at an earlier time containing peers Alice and Bob. Subsequently, P2P manages the protocols for the traditional communication depicted as the seven OSI layers shown. The actual processes during message exchange between Alice and Bob occur invisibly to the logical layer that manages their content exchange. In fact, in our target IoT environments, Alice and Bob are anonymized and only their information resource that brought them together remain as identifier of their exchange. As members of P2P, their shared P2P interest is a superset of their shared interest in a common information resource at the logical level.

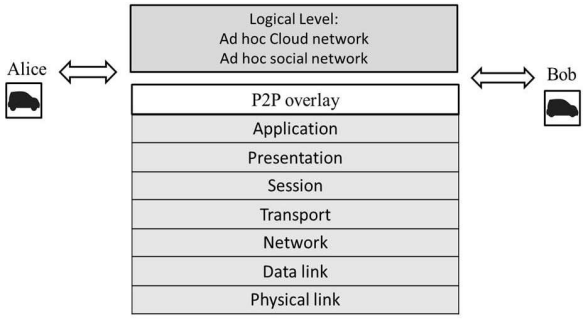

Figure 3. Spectrum of logical versus traditional communication layers

Policies have been prevalent in specifying network behavior and recently they are used for specifying IoT management [Singh,-2016]. Policies are not only essential for encapsulating global constraints for IoT, with tracking and enforcement, they are inevitable for privacy, security, and myriad legal concerns that is on the horizon for regulation and accountability of rampant IoT devices and networks.

IV. CONCLUSIONS

We are taking the position that advances in communication networking must be interwoven with the social networking principles and driven by policies that flexibly adjust the interaction patterns among internet of things. We have provided basic high-level steps for a combined framework as an enabling strategy to accommodate cohesive environments.

REFERENCES

[1] S. Alqithami, H. Hexmoor, 2014. Modeling Emergent Network Organizations, Web Intelligence and Agent Systems, Vol. 12, No. 3, pp. 1570-1263, IOS.

[2] S. Alqithami, H. Hexmoor, 2015. Ubiquity of Network Organizations: Paradigmatic Perspective and Synergistic Effect, In proceedings of Collaborative Technologies and Systems, IEEE Press.

[3] L. Atzori , A. Iera, G. Morabito, G., M. Nitti, 2012. The Social Internet of Things (SIoT) – When Social Networks meet the Internet of Things: Concept, Architecture and Network Characterization, Journal of Computer Networks 56, pp. 3594–3608, Elsevier.

[4] P. Chamoso, F. Prieta, J.. Francisco de Paz, J., J.M., Corchado, 2015. Swarm Agent-Based Architecture Suitable for Internet of Things and Smart-cities. In Distributed Computing and Artificial Intelligence, 12th International Conference, Springer Pub.

[5] H. Hexmoor, 2016. Compelling Use Cases for the Internet of Things, In International on Internet Computing and Internet of Things, Las Vegas, NV.

[6] H. Hexmoor, H., B. Gupta, 2017. Social Life Amidst the Internet of Things: Using P2P and Social Connectivity, In Proceedings of 32nd International Conference on Computers and Their Applications (CATA), Hawaii.

[7] P. Hinds, T. Roberts, H. Jones, 2004. Whose Job Is It Anyway? A Study of Human–Robot Interaction in a Collaborative Task, Journal of Human-Computer Interaction, Volume 19, pp. 151–181, Lawrence Erlbaum Associates pub.

[8] G. Fortino, A. Guerrieri, W. Russo, C. Savaglio, 2013. Integration of Agent-based and Cloud Computing for the Smart Objects-oriented IoT, In Proceedings of the 2014 IEEE 18th International Conference on Computer Supported Cooperative Work in Design, IEEE.

[9] M. Gerla, E.K. Lee, G. Pau, U. Lee, 2014. Internet of Vehicles: From Intelligent Grid to Autonomous Cars and Vehicular Clouds, IEEE World Forum on Internet of Things (WF-IoT).

[10] L. Hou, S. Zhao, S., X. Xiong, K. Zheng, 2016. Internet of Things Cloud: Architecture and Implementation, in IEEE Communications Magazine, pp. 32-39, IEEE Press.

[11] C. Hu, W.P. Tay, W.P., Y. Wen, 2012. Cloud robotics: architecture, challenges and applications, IEEE network Magazine, Vol. 26, No. 3, pp. 21-27, IEEE press.

[12] E. Lee, 2008. Cyber Physical Systems: Design Challenges, University of California, Berkeley Technical Report No. UCB/EECS-2008-8. Retrieved 2016-07-08.

[13] D. Kreutz, P. Esteves, S. Azodolmolskey, 2015. Software-Defined Networking: A Comprehensive Survey, in IEEE Spectrum, Vol. 103, No. 1, pp. 14-76, IEEE press.

[14] E. K. Lee, M. Gerla, S.Y. Oh, 2014. Vehicular Cloud Networking: Architecture and Design Principles, in IEEE Communications Magazine, pp. 148-155, IEEE press.

[15] F. Michahelles, P. Probst, 2012. Object Circles: Modeling Physical Objects as Social Relationships, In Proceedings of the 11th International Conference on Mobile and Ubiquitous Multimedia, ACM press.

[16] J. Singh, T. Pasquier, J. Bacon., J. Powles, R. Diaconu, D. Eyers, 2016. Big ideas paper: Policy-driven middleware for a legally-compliant Internet of Things. In Proceedings of the 17th Annual Middleware Conference, ACM press.