Reliability for Emergency Applications in Internet of Things

Nourhene Maalel, Enrico Natalizio, Abdelmadjid Bouabdallah, Pierre Roux, Mounir Kellil

▶ **To cite this version:**

Nourhene Maalel, Enrico Natalizio, Abdelmadjid Bouabdallah, Pierre Roux, Mounir Kellil. Reliability for Emergency Applications in Internet of Things. IEEE International Conference on Distributed Computing in Sensor Systems DCOSS, May 2013, Cambridge, MA„ United States. pp.361-366, 10.1109/DCOSS.2013.40 . hal-00863169

HAL Id: hal-00863169
https://hal.science/hal-00863169

Submitted on 20 Sep 2013

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Reliability for emergency applications in Internet of Things

Nourhene Maalel*†, Enrico Natalizio†, Abdelmadjid Bouabdallah†, Pierre Roux*, Mounir Kellil*
*CEA, LIST, Communicating Systems Laboratory, F-91191 Gif-sur-Yvette, France
†UTC, Heudiasyc Laboratory, UMR CNRS 6599, Compiègne, France
*name.surname@cea.fr, †name.surname@hds.utc.fr

***Abstract*— This paper addresses the Internet of Things (IoT) paradigm, which is gaining substantial ground in modern wireless telecommunications. The IoT describes a vision where heterogeneous objects like computers, sensors, Radio-Frequency IDentification (RFID) tags or mobile phones are able to communicate and cooperate efficiently to achieve common goals thanks to a common IP addressing scheme. This paper focuses on the reliability of emergency applications under IoT technology. These applications' success is contingent upon the delivery of high-priority events from many scattered objects to one or more objects without packet loss. Thus, the network has to be self-adaptive and resilient to errors by providing efficient mechanisms for information distribution especially in the multi-hop scenario. As future perspective, we propose a lightweight and energy-efficient joint mechanism, called AJIA (Adaptive Joint protocol based on Implicit ACK), for packet loss recovery and route quality evaluation in the IoT. In this protocol, we use the overhearing feature, characterizing the wireless channels, as an implicit ACK mechanism. In addition, the protocol allows for an adaptive selection of the routing path based on the link quality.**

Keywords—IoT; routing protocol; reliability

I. INTRODUCTION

Thanks to technology innovation, wireless broadband connectivity is turning out to be affordable and ubiquitous. This advance brings about the proliferation of connected devices through internet which interact and collaborate to accomplish a common task. This new paradigm is called Internet of Things (IoT) [1]. The major strength of the IoT idea is incontestably the high impact it will have on our daily life. Its application covers a variety of domains ranging from transport, agriculture, tracking, and defense to smart environments like homes and buildings [2].

However, "Things" may face a number of challenges that can hamper their widespread exploitation [3]. A network of things has to be self-adaptive and resilient to communication errors by providing efficient mechanisms for information distribution especially in the multi-hop scenario. These requirements have to be satisfied in an architecture that can be constrained by limited processing capabilities, scarce energy resources and unreliable communication channels [4]. In particular, in a typical harsh environment, the radio signal is often affected by interference; medium access conflicts, multipath fading, shadowing etc. These problems may result in significant packet losses. Moreover, the success of any application (particularly mission-critical ones like life-care data and alarms) requires the delivery of high-priority events to sinks without any loss on the path from the original sources to the final destination [5]. These constraints emphasize the need for an energy efficient, scalable and reliable data transport system.

Data retransmission has been considered as one of the most common schemes [6-7] for improving transmission reliability. The usage of ACK/NACK messages is the basic method used to assess the necessity of retransmission. Nevertheless, such a method generates an extra traffic, which causes an additional overhead that is not suitable in a highly constrained and error prone environment. Accordingly, an alternative solution should be found to deal with retransmissions without wasting bandwidth.

In this paper, we define a joint reliable and energy-efficient mechanism, called AJIA (Adaptive Joint protocol based on Implicit ACK), for packet loss recovery and route quality evaluation. In this

protocol, we transform the overhearing feature, which is usually considered as a drawback [8], because it provokes battery depletion, into an advantage for implicit ACK. We elaborate a lightweight protocol for data loss recovery, which allows high resource constrained nodes to achieve reliable data transmission. Our energy efficient approach uses the most consistent link and exploits the resource diversity of the IoT.

The remainder of this paper is organized as follows: the next section gives an overview of the concept of IoT. The next one summarizes the background and the challenges of the IoT paradigm, section 4 details our proposed protocol AJIA, and finally section 5 concludes this work.

II. INTERNET OF THINGS

A. *Concept*

The IoT designates a novel paradigm that connects the pervasive heterogeneous variety of things around us to the Internet and among themselves. The IoT is foreseen to be 'a self-configured dynamic global network infrastructure with standards and interoperable communication protocols where physical and virtual things have identities, physical attributes, and virtual personalities, and are seamlessly integrated into the information infrastructure' [9].

Since this concept has emerged, we have seen the deployment of a new generation of networked smart objects with powerful abilities (typically communication, sensing and action). These capabilities enable to cover various applications ranging from healthcare to smart environments, from monitoring to transportation [10-12], etc. All these applications' success relies on the data collected from distributed smart 'network enabled' objects and the reliability of the used infrastructure for data transmission.

B. *IoT in emergency applications*

As mentioned above, emergency applications require an immediate response to any alarm which involves a continuous supervision of the alarm state. Communicating objects in the IoT provide complete visibility of the resources to the administrator of the system. In building monitoring, for example, such visibility enables instant reaction to any event by transferring real-time information about the occurrence and extension of an accident (such as a fire) outside the building [2]. The reliable transmission of parameters, such as temperature and smoke ingress, can greatly increase awareness and reactivity of the first responders [2].

In summary, the inclusion of the IoT concept into emergency application will open new perspectives by identifying the 'things', achieving sensing tasks and building low cost and reliable solutions and services.

III. BACKGROUND & CHALLENGES

Currently, many challenging topics have to be addressed in the IoT. We can summarize these challenges by:

- Allowing a full interoperability of the interconnected devices despite their heterogeneity.
- Enabling an autonomous behavior and a self adaptation to the environment and network unreliability by providing a high degree of smartness.
- Guaranteeing privacy and security issues for all applications.
- Elaborating energy efficient and scalable solutions.

Several standards are currently involved in the development of solutions for IoTs fulfilling the highlighted technological requirements and acting as a bridge between the physical world and the Internet for the IoT. The most used are ZigBee [14] and 6LowPAN [13]. Both of them are implemented on top of the IEEE 802.15.4 standard [15] which is a protocol designed for low data rate, and low power consumption network. In this paper, we give special consideration to reliability issues and more particularly to the reliable data transmission paradigm, which can be extremely critical in some emergency application. Indeed, a rapid response is required in critical situations (fire detection, terrorist attack, etc) to avoid serious damages or even loss of human lives. That is the reason why prompt awareness and reliable decision-making support are important factors for minimizing such dangers. More concretely, the varying environment and requirements during an emergency require the ability to dynamically react in a rapid and correct way. The wrong transmission of such relevant data, due to link failure or congestion, by nodes can provoke harmful consequences. Therefore, adequate mechanisms need to be developed and implemented in order to reconstruct new paths when established ones break.

IV. PROPOSED PROTOCOL

C. Overview of the mechanism

Throughout this paper, we focus on elaborating an efficient packet loss control mechanism with implicit acknowledgments. Our protocol tackles the link failure and packet loss problem, by proposing a reliable and energy-efficient error control protocol in a limited computational resources environment. Our idea stems from the overhearing characteristic of wireless communication as shown in Figure 1. When a node transmits a packet, nodes in its neighborhood overhear the packet transmission even if there are not the intended recipients, due to the broadcast nature of the wireless channel.

Our solution uses this overhearing characteristic instead of the acknowledgment messages to guarantee reliability in the network. Moreover, when a packet loss is detected, retransmission is carried out on the most reliable link between the node that sent the (lost) packet and its one-hop neighbors. The reliability of links is defined through a metric based on the link history and the link quality indicator (LQI) which will be detailed in the next subsection. Besides, the device resource heterogeneity in IoT is exploited to load balance the traffic and share the current workload. Indeed, nodes with available resources are the most involved in retransmission issues.

To achieve these goals we have taken a different approach in comparison to traditional end-to-end error recovery mechanisms, where only the final destination node is responsible for detecting loss and requesting retransmission. We propose a hop-by-hop packet loss recovery mechanism, in which intermediate nodes also take responsibility for loss detection and recovery. This approach essentially segments multi-hop forwarding operations into a series of single hop transmissions that eliminate error accumulation. Intuitively, the hop-by-hop approach is more scalable and capable to recover from loss.

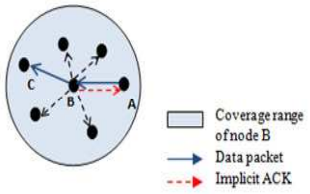

Figure 1 Implicit ACK for the transmission from node A to B

D. Network model and assumptions

We consider a dense set of randomly distributed objects. Our objective is to provide a reliable retransmission scheme that takes into consideration the link consistency without inducing the extra overhead caused by acknowledgement messages. Before discussing the details of our protocol, we need to clarify our assumptions:

-We assume that the network is composed of heterogeneous objects such as sensors, actuators, mobile phones, etc, which have different transceiver characteristics and are randomly distributed in a limited environment.

- All the devices have sufficient resources to perform sensing, computing, and communication activities.

- We consider a many-to-one traffic pattern where source nodes send data to the sink.

- Data packets are randomly generated and transmitted to the sink node.

- We assume that nodes are stationary during their lifetime and able to record the performance of the link between themselves and their neighboring nodes, in terms of the ratio *packet lost/packets sent*.

- We adopt a basic routing scheme, where a packet gets one-hop closer to the sink after each transmission. This is made possible by assigning to each node a level corresponding to its hop-distance from the sink. Data is transmitted level by level toward the sink. When different nodes are at the same distance from the sink, the next hop is chosen according to its resources: in the routing decision, nodes will privilege neighbors whose energy is not limited by their battery (electrical plugged devices), in order to limit the energy expenditure of electrically unplugged devices.

- We assume that the collection of data from a node to the sink must be completed within a specified time. If the packet does not reach the sink within this time limit, it is dropped and considered as it has been lost.

- We assume to have a symmetrical channel, so that both the endpoints of the channel will keep an identical history of link performance. Link state is set to up or down after each packet transmission depending on the reception/loss of the packet at the receiving endpoint of the link. We consider that a link state is up if a packet is correctly transmitted through it, and down otherwise. The channel state history is made up by the set of evaluations performed on the state of a channel. Since the

channel state is binary, a simple count of the number of states (up/down) suffices to fully describe its history.

E. Algorithm steps

Our work proposes a reliable data transfer by using link reliability based on implicit acknowledgments. The motivation behind our protocol is to ensure low latency, while minimizing the loss recovery cost by using localized data recovery among one hop neighbors.

Our algorithm comprises an initialization phase followed by three steps: message relaying, lost message detection and selective recovery:

1) Initialization phase

The initialization phase starts with the construction of a spanning tree for ordinary routing operations. To perform this task, we assign levels to nodes. A level corresponds to the hop-distance of the node from the sink and data will be transmitted level by level toward it.

Besides, we maintain a consistent history of the state of the different links. The channel history will be used to elaborate our AJIA metric used in the recovery mechanism, which will be explained in the next subsection. By using the mentioned assumptions, we can characterize the link reliability by the probability of link failure based on the history. Let A and B be two communicating nodes, n_{up} be the number of successful transmissions through the link AB and n_{down} be the number of failed transmissions. We denote the link failure probability, P_{hist}, as it follows:

$$P_{hist}(A,B) = \frac{n_{up}}{n_{up} + n_{down}} \quad (1)$$

2) Message relaying

Packets are forwarded hop by hop to get closer to the sink. Intermediate nodes keep the $packet_{Id}$ in their buffer during T_{col} corresponding to the maximum delay allowed to transmit a packet from a source to the sink. Neighbors that receive this packet check their local data cache to discard any replica. If the packet is received for the second time, it is automatically dropped to avoid message duplication.

3) Lost message detection

The lost message detection is achieved thanks to the overhearing mechanism. Let us assume that node A sends a packet $packet_{Id1}$ to node B. After the transmission, node A awaits T_{wait} instants of time overhearing node B's transmission, in order to check whether the packet has been well transmitted or not. By localizing loss events, this mechanism segments the multi-hop forwarding operations into a series of single hop transmission processes, which is effective in highly error-prone environments. Upon sensing the channel, if node A does not hear node B transmitting the packet $packet_{Id1}$ to its next hop, it becomes aware that the packet has been lost and that a retransmission is required.

4) Selective recovery

Once a packet loss is detected, the AJIA mechanism relies on its routing metric to choose the best next hop for the packet retransmission. AJIA metric evaluates and assigns costs to network links, and then it determines the most suitable node to act as a relay. The metric component of AJIA evaluates links according to 3 parameters:

-The history of the link presented in the previous subsection.

-The Link Quality Indicator (LQI) is a metric of the current received signal quality. By using the 802.15.4 standard [15], we have access to the LQI of the channel between neighboring nodes in the network. This measurement is included into the MAC header of each received packet. The use of the LQI score function ensures a certain level of adaptability to the environmental conditions. In fact, it expresses the real quality of the link. The implementation of our adaptive routing is accomplished by considering the LQI, which is considered as a so-called "stigmergic" variable (i.e. a variable that contains the information used by nodes to communicate indirectly). The LQI variables are defined and used by nodes to adaptively change the way they build routing path. Any change in this value may induce a change in the preferred direction towards the sink.

-The resources of the node: the heterogeneous nature of the IoT infers various level of resources consumption for different devices. While sensor nodes are constrained by their batteries, other devices like computers or phones are not limited by resources scarcity. This is the reason why we pay special attention to this parameter when we choose the best next hop and we exploit the network diversity to preserve objects energy.

Besides, LQI experiences frequent fluctuations in highly interfered environment. Hence, we consider statistics (average number of lost packet per link) as a basis to assess the reliability of links. For this reason, we have decided to weight the AJIA metric by the link failure probability given by our

probabilistic history model, P_{hist} (A,B) described in equation (1). Therefore, even if the last recorded value of LQI does not match the real state of the link, the history will correct it. Let us state that P_{hist} (A,B) is set to 1 at the beginning, and during a fixed time T_{init}, before having a real history. In fact, at the establishment of the process, we do not have sufficient feedback to assess the reliability of a link.

We need to recall here that we assumed that the first parameter to consider for transmitting a packet from node A to the sink is the number of hops. Consequently, only the one-hop neighbors with a level value lower than that of A (nodes which are closer to the sink) will be candidates to retransmit the packet.

To do so, AJIA assigns a cost to each ling, which is given by the following expression:

$$AJIA\ (A,B) = K * e^{-age} * LQI_{AB} + \frac{1}{P_{hist\,AB}} + E \qquad (2)$$

Where LQI_{AB} denotes the link state indicator between nodes A and B and *age* corresponds to the delay since the LQI value has been recorded. The exponential function provides a decreasing function according to the age, which means that more recent values of LQI are considered as more significant. The P_{hist} represents the probability of link success between nodes A and B. K is a constant used to weight the equation. E is related to the resource available at the device. It varies from 1 to 10, where 1 means a device with a limited battery and 10 indicates a device with limitless resource (a computer plugged into the electrical network).

Once this metric is calculated for all the candidate nodes closer to the sink, node A choices the node with the highest AJIA metric to retransmit the lost packet. Indeed the reliability of the link is proportional to this AJIA metric: the higher the metric, the more reliable the link. This process is repeated until the packet is received (an implicit ACK is received) or until a specific timer expires and ends the packet lifetime. In this case, the packet is dropped and considered as lost.

V. Conclusion

To meet the stringent requirement of reliably transmitting data in the IoT, we propose a reliable protocol for data transmission adapted to the emergency application. Our protocol is designed to operate in the IoT environment characterized by a huge diversity of devices resources. It relies on implicit acknowledgements to detect transmission error and elaborates a routing metric to designate the best link minimizing packet loss probability.

For future work, we intend to evaluate our protocol via simulations to assess its effectiveness in terms of packet loss and energy efficiency and in comparison to different approaches. We also plan to examine probabilistic models permitting to predict the state of our objects in order to choose the most adapted link to transmit packets.

VI. References

[1] L. Atzori, A. Iera, G. Morabito, "The Internet of Things: a survey", Computer Network, 54, pp. 2787-2805, 2010.

[2] L. Yang, S.H. Yang, L. Plotnick, "How the internet of things technology enhances emergency response operations", Technological Forecasting & Social Change, 2012.

[3] K.Srinivasan, P.Dutta, A.Tavakoli, "An empirical study of low-power wireless", ACM Trans. Sen. Netw., 6(2), pp. 1–49, Feb. 2010.

[4] M. Nassr, J. Jun, S. Eidenbenz, A. Hansson "Scalable and reliable sensor network routing: Performance study from field deployment," in The 26th IEEE INFOCOM, pp. 670–678, 2007.

[5] Y. Xiao, X. Li, Y. Li, and S. Chen, "Evaluate reliability ofwireless sensor networks with OBDD," in IEEE International Conference on Communications (ICC '09), pp. 1–5, 2009.

[6] S. J. Park, R. Vedantham, R. Sivakumar, and I. F. Akyildiz, "A scalable approach for reliable downstream data delivery in wireless sensor networks", in Proc. of the 5th ACM MobiHoc, pp. 78–89, 2004.

[7] C. Taddia and G. Mazzini, "On the retransmission method in wireless sensor networks", in Proc. of VTC 2004-Fall, 2004.

[8] J. Hui, D. Culler, S. Chakrabarti, "6LoWPAN: Incorporating IEEE 802.15.4 Into the IP Architecture" (IPSO) Alliance, 2009.

[9] S. Singh, C. S. Raghavendra, "PAMAS – Power aware multi-access protocol with signaling for adhoc networks", ACM

SIGCOMM Computer Communication Review, 1998.

[10] European Commission, “Internet of things strategic research roadmap”, 2009.

[11] A. Oztekin, F.M. Pajouh, D. Delen, L.K. Swin, “An RIFD network design methodology for asset tracking in healthcare”, Decis. Support Syst., 49, pp. 100–109, 2010.

[12] C.W. Thompson, F. Hagstrom, “Modeling healthcare logistics in a virtual world”, IEEE Internet Comput., 12(5), pp. 100–104, 2008.

[13] A. Llic, T. Staake, E. Fleisch,” Using sensor information to reduce the carbon footprint of perishable goods”, IEEE Pervasive Comput.: 8(1), pp. 22–29, 2009.

[14] N. Kushalnagar, G. Montenegro, C. Shumacher, “IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)”, RFC4919.

[15] ZigBee Alliance, Electronic Text at, http://www.zigbee.org.