An Adaptive Learning Approach for Fault-Tolerant Routing in Internet of Things

Sudip Misra
School of Information Tech
Indian Institute of Technology
Kharagpur, India
smisra@sit.iitkgp.ernet.in

P. Venkata Krishna, Harshit Agarwal
School of Computing Science and Engineering
VIT University
Vellore, India
parimalavk@gmail.com, harshit.agarwal@live.com

Anshima Gupta
School of Information Technology and Engineering
VIT University
Vellore, India
anshimagupta@hotmail.com

Mohammad S. Obaidat
Fellow of IEEE & Fellow of SCS
Dept. of Computer Science
Monmouth University, NJ, USA
obaidat@monmouth.edu

***Abstract*—Internet of Things (IOT) is a wireless ad-hoc network of everyday objects collaborating and cooperating with one other in order to accomplish some shared objectives. The envisioned high degrees of association of humans with IOT nodes require equally high degrees of reliability of the network. In order to render this reliability to IOT networks, it is necessary to make them tolerant to faults. In this paper, we propose mixed cross-layered and learning automata (LA)-based fault-tolerant routing protocol for IOTs, which assures successful delivery of packets even in the presence of faults between a pair of source and destination nodes. As this work concerns IOT, the algorithm designed should be highly scalable and should be able to deliver high degrees of performance in a heterogeneous environment. The LA and cross-layer concepts adopted in the proposed approach endow this flexibility to the algorithm so that the same standard can be used across the network. It dynamically adopts itself to the changing environment and, hence, chooses the optimal action. Since energy is a major concern in IOTs, the algorithm performs energy-aware fault-tolerant routing. To save on energy, all the nodes lying in the unused path are put to sleep. Again this sleep scheduling is dynamic and adaptive. The simulation results of the proposed strategy shows an increase in the overall energy-efficiency of the network and decrease in overhead, as compared to the existing protocols we have considered as benchmarks in this study.**

Keywords-IOT; Cross-Layer Design; Learning Automata; Fault-tolerant routing;

I. INTRODUCTION

IOT refers to a nexus of customary and conventional objects connected in the form of an internetwork. The primary concept behind this new technology is the pervasive presence of these objects such as RFID around us interacting and collaborating with each other to attain mutual goals. Of course in order to communicate with one another, the network-enabled objects need common protocols and standards for communication.

Indubitably, IOT is envisioned to have huge influence on a variety of aspects of our everyday life [1]. It is likely to emerge as a new technology capable of playing a prominent role in a wide range of applications ranging from basic domestic assistance to intelligent automated industrial systems. From the bird's eye view, IOT is a self-configuring wireless network which integrates the physical world with the world of Internet [2]. It has the potential to equip humans with the ability to have high degrees of control over physical objects. It will enable centralized unified control which is extended to almost every object in the proximity.

The huge interconnection requirement between the nodes in IOT will require the enabling of huge centralized/decentralized database of objects across the globe. It will require a unique addressing system so that each device can be uniquely identified. IOT draws lot of similarity with the current day Internet, but it has significantly high level of diversity and enormous number of communicating devices. IOT devices share information about their states and other vital factors which imparts them with essential, though unique, characteristics such as self-management, self-decision making and self-governance [3]. The aspects of cooperation endows them autonomy and intelligence.

An IOT is conceived to be open and self-assimilating internetwork. These kinds of internetworks are highly prone to faults and security threats [4]. These faults, if not handled properly, may lead to serious network downtime. Faults tend to degrade the network performance and affect the network's operation time by introducing unnecessary overheads. Faults can occur due to a variety of factors. To generalize, they can be classified into two major categories namely hardware-based and software-based. The more critical the application of network would be, the more severe would be the implications because of such faults. In case of IOTs, due to their large scale, these faults have magnified repercussions. To make IOT a robust, reliable and dependent technology, it is necessary to adopt a strategy to avoid and counter these faults.

In this paper, we focus on the fault-tolerance aspects in routing. We propose a learning automaton (LA) [5-7] based intelligent fault-tolerant routing algorithm for IOT. We introduce the concept of cross-layering [8-9] to optimize the energy saving while handling the faults at the same time. LA is an intelligent and adaptive approach which takes decision based on the feedback from the environment. It reiterates this process to choose the most optimized action. This paper is inspired from the work presented in [5], where Misra et al. proposed an LA-based fault-tolerant routing algorithm for mobile ad hoc networks (MANETs). We have modified the existing approach to meet the specifications of IOT-like networks and tested it by simulating it using ns-2.

II. MOTIVATION

Our literature survey shows that the fault-tolerance aspects on routing in IOTs require serious attention. As discussed in Section I, an IOT consists of huge number of devices, most of which are enabled by RFID or other similar type of devices. Such kinds of objects have low computational capabilities due to limited resources and is highly prone to both software and hardware faults. For this type of network to be functional, it is essential to have some fault-countering strategy in place. Not only in respect of computational power, are these devices also constrained in terms of energy. Therefore, a fault-tolerant approach which considers energy as the important factor while taking routing decisions is a crucial necessity. To handle the complexities of IOT it is desired to have an intelligent and adaptive solution.

The major challenge involved in designing network protocol for IOT is the enforcement of same standards for a variety of devices of which IOT is composed of. As these devices vary primarily in their capabilities, following a common standard for all is likely to cause considerable performance degradation. But having different communication standard for different set of devices is impractical and unfeasible as well. Firstly, defining so many different standards is unrealistic and, secondly, achieving flawless interoperability among these protocols is unattainable. So, in order to tackle these issues, we devised an approach which is adaptive in nature.

We employ LA in the proposed solution which constrains all the devices to follow the same protocol and simultaneously providing customization capabilities for every device. The proposed algorithm adjusts various parameters based on the environment in which the nodes are operating. Since we are following the same standard, the interoperability issue is obviated. To further optimize the performance, the cross-layer model helps by letting the algorithm perform fault-tolerant routing while being aware of the energy of nodes lying in the route, thereby empowering it with the competency to avoid faults that might take place due to deprivation of energy. A goodness value is calculated for every possible path between a source and destination. This value denotes the fitness of a path or its suitability to carry out communication. One with the highest goodness values is preferred.

III. LEARNING AUTOMATA

The theory of LA centers on the notion of an "*automaton,*" which is a self-operating machine or a mechanism that responds to a sequence of instructions in a certain way, so as to achieve a certain goal. The automaton either responds to a pre-determined set of rules, or adapts to the environmental dynamics in which it operates. The term "*learning*" refers to the action of procuring knowledge and modifying one's behavior based on the experience earned. Thus, the learning automata adapt to the responses from the environment through a series of interactions within them. The automata, then, attempt to learn the best action from a set of possible actions that are offered to them by the random stationary or non-stationary environment in which they operate. The automata, thus, act as decision makers to arrive at the best action.

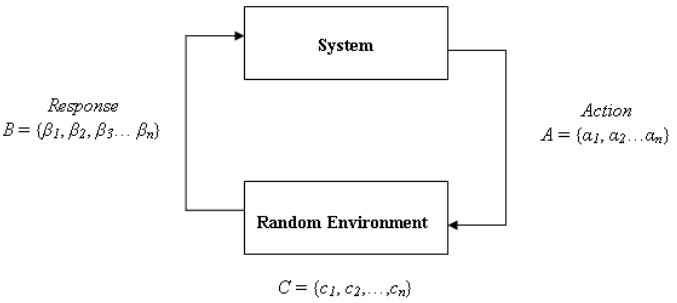

Fig. 1 The learning automaton

LA can be used in optimization problems, since an automaton in LA selects that action which is more likely to be awarded by the environment. Over a period of time, LA learns from its actions and chooses an optimal solution. A comprehensive overview of LA can be found in the classic text by Narendra and Thathachar [6] and in the recent book chapter by Oommen and Misra [7].

A. The Automaton

The automaton can be represented as a quintuple represented as $\{Q, A, B, F, H\}$, where [10]:

- Q is the finite set of internal states $Q = \{q_1, q_2, q_3 \ldots q_n\}$ where q_n is the state of the automaton at instant n.
- A is a finite set of actions performed by the automaton. $A = \{\alpha_1, \alpha_2 \ldots \alpha_n\}$ where α_n is the action performed by the automaton at instant n.
- B a finite set of responses from the environment. $B = \{\beta_1, \beta_2, \beta_3 \ldots \beta_n\}$ where β_n is the response from the environment at an instant n.
- F is a mapping function. It maps the current state and input to the next state of the automaton. $Q \times B \rightarrow Q$.
- H is a mapping function. It maps the current state and response from the environment to determine the next action to be performed.

B. The Environment

The environment corresponds to the medium in which the automaton functions. Mathematically, an environment can be

abstracted as a triple $\{A, B, C\}$. A, B, and C are defined as follows [10]:

- $A = \{\alpha_1, \alpha_1, \ldots, \alpha_n\}$ represents a finite input set;
- $B = \{\beta_1, \beta_2, \ldots, \beta_n\}$ is the output set of the environment; and
- $C = \{c_1, c_2, \ldots, c_n\}$ is a set of penalty probabilities, where element $c_i \in C$ corresponds to an input action α_i.

We now provide a few important definitions used in the field of LA. Given an action probability vector **P** (t) at time t, the *average penalty* is defined as [10]

$$M(t) = E[\beta(t) | P(t)] = \Pr[\beta(t) = 1 | P(t)]$$

$$= \sum_{i=1}^{r} \Pr[\beta(t) = 1 | \alpha(t) = \alpha_i] \times \Pr[\alpha(t) = \alpha_i]$$

$$= \sum_{i=1}^{r} c_i p_i(t). \quad (1)$$

The average penalty for the "pure-chance" automation is given by [4]

$$M_0 = \frac{1}{r} \sum_{i=1}^{r} c_i. \quad (2)$$

As $t \to \infty$ if the average penalty $M(t) < M_0$, at least asymptotically, the automaton is generally considered to be better than the pure-chance automaton. $E[M(t)]$ is given by [10]

$$E[M(t)] = E\{E[\beta(t) | P(t)]\} = E[\beta(t)]. \quad (3)$$

IV. Cross Layer Design

The need to have an energy-aware fault-tolerant routing motivated us to choose cross-layer design. The traditional OSI model does not allow the interaction among the different layers of the network stack. However, to improve performance or to increase services, this rigid model has been challenged by the researchers [11-12]. The conventional model fails to serve all the requirements of wireless network. IOT generally is composed of small devices such as RFID, which are low in energy. So, energy limitation is a major design constraint for any protocol in IOT. Therefore, to address this limitation, cross-layer design has been employed, which permits the access to the energy statistics. As the energy related information is available with physical layer, this information is passed on to the network layer via shared data structure. The fault tolerant routing algorithm stationed at network layer uses this energy knowledge to take better decisions hence deliver better performance. Fig. 2 gives the diagrammatic representation of the cross-layer design component.

V. System Model

We represent a wireless network using a graph W = (V, E), where V represents the set of vertices and E the set of edges. The vertices are the nodes in the network and the edges are the wireless links in between the wireless nodes. A path is a set of vertices connected to each other from a vertex (which can also be source) to destination (sink). Faults can occur unpredictably in any node in the network. We assume all links in the network to be bidirectional, i.e., if $(v_i, v_{i+1}) \rightarrow E$, then $(v_{i+1}, v_i) \rightarrow E$ also exists. Each node 'v' has two components: a routing component and an LA component. Each node's LA component functions independently of others and shares updates through an update table maintained at the routing component which shares LA information through the neighbor nodes. Apart from network layer inputs it uses the data from the physical layer while rewarding or penalizing the path. Fig. 3 depicts the proposed system model outline.

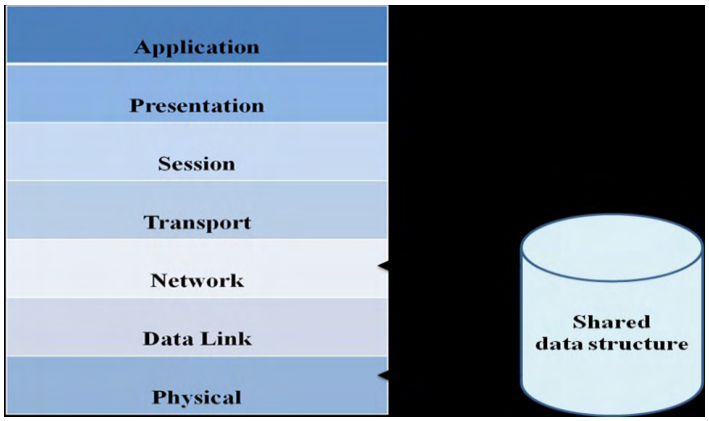

Fig. 2. Cross-Layer Design

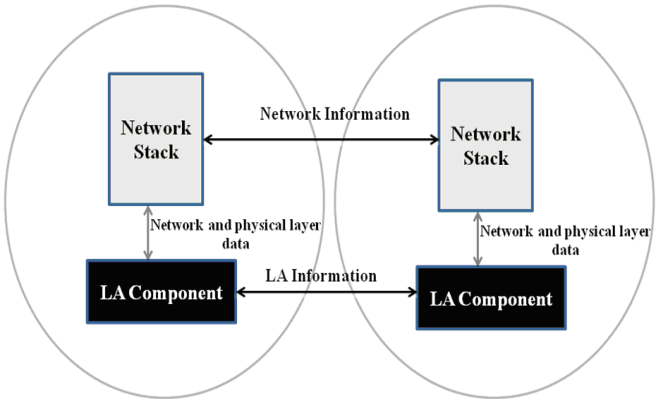

Fig. 3. System-model

VI. Algorithm

The proposed algorithm, named as Cross-Layer-Based Adaptive Fault-Tolerant Routing Algorithm for IOTs (i-CLAFTRA) uses multipath for the transmission of data between a pair of communicating devices. During the data transmission, the goodness value [5] of the various paths available is calculated using reward/penalty scheme of LA. If the goodness value of the current path is above the threshold, then it continues the transmission using the same path otherwise the path with highest goodness value is chosen for further transmission of packets. The remaining nodes that are

not lying on any currently being used path are put to sleep to save energy. The goodness value of the path is continuously and dynamically updated using the underlying reward/penalty scheme by LA.

A. Reward/Penalty Scheme

As described earlier, each node has a learning automaton stationed in it. Therefore, the automaton keeps a check on the delivery of the packet sent through it. If the packet delivery is reported to be successful then the stationed LA increments the value of the goodness value of that particular node. The increment is the sum of a constant R, the reward constant and a function of energy remaining level of the node. The node with higher level of energy remaining will get the higher reward as it is better to select the nodes with the more energy as they will deliver better operation time.

To calculate the goodness value of the path, we take the commulative sum of the goodness values of the nodes lying in that path. Once the computation of the goodness value is completed, it is then compared with the threshold and accordingly the most suitable path is selected. The nodes of the remaining unused path areput to sleep. This increases the network lifetime.

B. Sleep/Wake up Scheme

As soon as a fault is detected in the currently used path, then the path is switched to the alternative path with the next highest path goodness value. Other than this, if the goodness value of a path falls by 10%, then the source node will check if the alternate path is good enough (i.e., has goodness value higher than the currently used path) for data transmission, then it will use alternate path. If the goodness value of any of the alternate paths is not more than current path, then in such a case, it will continue using the current path.

In the given strategy, the nodes undergo sleep and wake-up, depending upon the goodness value of path which is different from S-MAC [13]. The higher the goodness values of a path, the more number of nodes will be active in that path, resulting in the path's greater suitability and higher reliability in transferring data. Since the proposed scheme dynamically controls the sleep scheduling of the nodes, this algorithm results in reduced overhead and less energy consumption.

The algorithm is shown by the pseudo-code below:

Algorithm: i-CLAFTRA

1. Initialize the LA parameters.
2. Using route discovery find path between source and destination.
3. Find optimal path between source and destination.
4. Put remaining nodes to sleep.
5. Packet delivery across the node----reward/penalize by altering the goodness value of the path.
6. Calculate the updated goodness value of node.
7. For every 10% drop in goodness value.
8. If(goodness value of current path> goodness value of alternate path)----use current path
9. else---switch to alternate path

VII. SIMULATIONS

We have performed simulations of the proposed solution, i-CLAFTRA, using ns-2 [14], and have compared its performance with the corresponding algorithms in ENFAT-AODV [13] and AODV [15]. The parameters used for ns-2 simulation are specified in Table 2.

TABLE 1: Simulation parameters

Parameter	Value
Number of Nodes	40-240
Speed	0-15 m/s
MAC	IEEE 802.11
Traffic type	CBR (at TCP-IP interface)
Terrain Dimensions	1200 m x 1000 m

A. Variation in average energy consumption with respect to mobility in the network

The aim of this experiment was to study the energy consumption by the network with varying percentage of mobile nodes.

Fig. 4 shows the variation in average energy consumption of i-CLAFTRA, AODV and ENFAT-AODV. It is observed from the graph that energy consumption by i-CLAFTRA is less than other protocols. i-CLAFTRA performs well because of the ability of learning automata adaptability and its sleep mechanism. Energy consumption in AODV remains constant as all nodes remain active and dissipate nearly same amount of energy. The average energy consumption by ENFAT-AODV increases as number of nodes increases as it has to spend more energy in maintaining the alternate path.

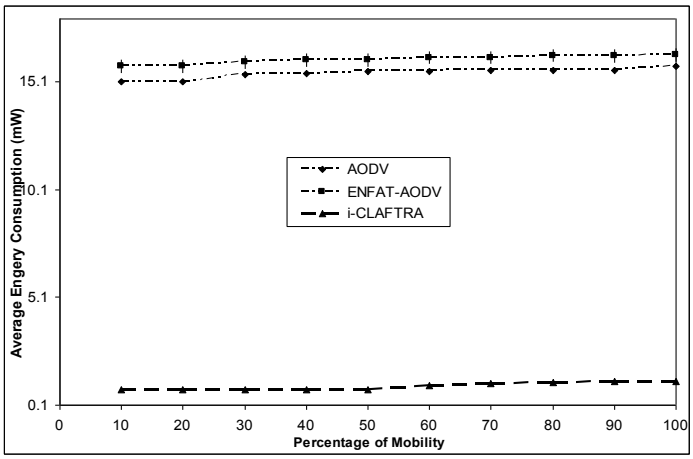

Fig. 4 Graph for average energy consumption versus percentage of mobility

A. Variation in packet delivery ratio with respect to percentage of mobility in the network

In this experiment, we examined the packet delivery ratio while varying the percentage of mobility in the network.

Fig. 5 shows the variation in packet delivery ratio with respect to percentage of mobility where pause time was kept constant at 300 sec. As depicted by the graph, the performance of the i-CLAFTRA is significantly better than its counterparts.

i-CLAFTRA's packet delivery ratio is affected by a very minor factor as the percentage of mobility increases. By percentage of mobility, we imply the fraction of mobile nodes of the total nodes in a network. As we know, IOT can have both mobile as well as stationary nodes at the same time, we have taken this parameter as one of the criteria for analyzing i-CLAFTRA's accomplishment. The increasing gap between the curve of i-CLAFTRA and other two curves shows the stability in the execution the proposed protocol has as compared to AODV and ENFAT-AODV.

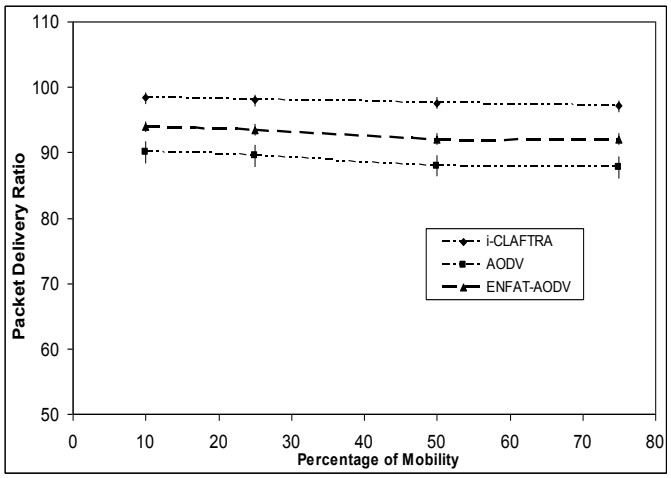

Fig. 5 Graph for percentage mobility versus packet delivery ratio in the network

VIII. CONCLUSION

The proposed protocol is a fault-tolerant routing protocol for IOT. The protocol has been designed using the LA and cross-layer design concepts. It has been designed to operate in the IOT like environment where the diversity of devices and the figure of devices are huge. The energy saving strategy ensures the longer operational lifetime for the network. Cross-layer design not only equips this algorithm with the ability to save power but also helps it in avoiding faults taking place due to paucity of energy. LA is stationed at each node to select the best path available among the multiple paths based on its goodness value. The goodness value of the path is updated using the reward/penalty scheme of LA. These parameters are well influenced by energy of the node lying in the path. So the path that has the least probability of fault occurrence is preferred. To summarize, this work provides an effective mechanism for fault tolerant routing for IOTs.

In the future, we want to evaluate this solution to assess its scalability and usefulness in a wide range of application domains.

ACKNOWLEDGEMENT

The work of the first author was supported in part by the Council for Scientific and Industrial Research (CSIR), New Delhi, India, Grant Ref. No. 22(0477)/09/EMR-II.

REFERENCES

[1] L. Atzori, A. Iera and G. Morabito, "The Internet of Things: A survey", *Computer Networks*, Vol. 54, No. 15, October 2010, pp. 2787-2805, ISSN 1389-1286, DOI: 10.1016/j.comnet.2010.05.010.

[2] O. Zhu, R. Wang; Q. Chen, Y. Liu and W. Qin, "IOT Gateway: BridgingWireless Sensor Networks into Internet of Things," *Embedded and Ubiquitous Computing (EUC), 2010 IEEE/IFIP 8th International Conference on* , vol., no., pp.347-352, 11-13 Dec. 2010 doi: 10.1109/EUC.2010.58.

[3] ITU Internet Reports, *The Internet of Things*, November 2005.

[4] S. Misra, P. V. Krishna, H. Agarwal, A. Saxena and M. S. Obaidat, "A Learning Automata Based Solution for Preventing Distributed Denial of Service in Internet of Things", *Proceedings of the International Conference on Internet of Things* (*iThings 2011*), Dalian, China, October 2011.

[5] S. Misra, P. V. Krishna, A. Bhiwal, A. S. Chawla, B. Wolfinger, and C.Lee, "A learning automata-based fault-tolerant routing algorithm for mobile ad hoc networks", *Journal of Supercomputing*, 2011-07-05, Springer Netherlands, Doi: 10.1007/s11227-011-0639-8.

[6] K. S. Narendra and M. A. L. Thathachar, *Learning Automata*, Prentice-Hall, 1989.

[7] M. A. L. Thathachar and P. S. Sastry, "Networks of Learning Automata", Kluwer Academic, 2003.

[8] V. Srivastava and M. Motani, "Cross-layer design: a survey and the road ahead," *IEEE Communications Magazine*, vol.43, no.12, pp. 112-119, Dec. 2005, doi: 10.1109/MCOM.2005.1561928.

[9] M. Conti, G. Maselli, G. Turi, S. Giordano, "Cross-Layering in Mobile Ad Hoc Network Design," *Computer*, vol. 37, no. 2, pp. 48-51, Feb. 2004, doi:10.1109/MC.2004.1266295.

[10] B. J. Oommen and S. Misra, "A Fault-Tolerant Routing Algorithm for Mobile Ad Hoc Networks Using a Stochastic Learning-Based Weak Estimation Procedure," *IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, 2006 (WiMob'2006).*, pp. 31-37, 19-21 June 2006, doi: 10.1109/WIMOB.2006.1696374

[11] S. Shakkottai, T. S. Rappaport and P. C. Karlsson, "Cross-layer design for wireless networks", *IEEE Communications Magazine,* vol.41, no.10, pp. 74- 80, Oct 2003.

[12] V. T. Raisinghani and S. Iyer, "Cross-layer feedback architecture for mobile device protocol stacks", *IEEE Communications Magazine*, vol.44, no.1, pp. 85- 92, Jan. 2006.

[13] Z. Che-Aron, W. F. M. Al-Khateeb and F. Anwar, "ENFAT-AODV: The fault-tolerant routing protocol for high failure rate Wireless Sensor Networks," *Proceedings of the 2nd International Conference on Future Computer and Communication* (*ICFCC*), pp.V1-467-V1-471, 21-24 May, 2010, doi: 10.1109/ICFCC.2010.5497747.

[14] ns-2: Network Simulator 2, http://www.nsnam.org

[15] C. Perkins, E. Belding-Royer and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing", IETF, RFC 3561, July 2003.