Hindawi Publishing Corporation
EURASIP Journal on Wireless Communications and Networking
Volume 2008, Article ID 386898, 9 pages
doi:10.1155/2008/386898

Research Article

A QoS-Aware Mesh Protocol for Future Home Networks Using Autonomic Architecture

Kaouthar Sethom, Tara Ali-Yahiya, Nassim Laga, and Guy Pujolle

Computer Science Laboratory, University of Pierre and Marie Curie–Paris6, 104 avenue du president Kennedy, 75016 Paris, France

Correspondence should be addressed to Tara Ali-Yahiya, tara.ali-yahiya@lip6.fr

Received 28 November 2007; Revised 30 March 2008; Accepted 15 July 2008

Recommended by Jong Hyuk Park

Autonomic networking is an emerging approach for the research community to engineer systems and architectures that will increase the quality of service (QoS) and robustness of future network architectures. In this article, we investigate the key concept of adding a knowledge plane to enable the automated control and management of home resources taking into account wireless mesh topology basis. This new supplementary plane helps to make an intelligent decision to select network paths that have sufficient resources to satisfy the QoS requirements of the admitted connections.

1. INTRODUCTION

The recent technology improvements in wireless communications and electronics have changed the traditional view of the home environment from a simple interconnection of few manually administered homogeneous devices to a complex infrastructure encompassing a multitude of different technologies (wired/wireless, mobile/fixed, and static/ad hoc, etc.), heterogeneous nodes (regarding variety of devices, size, capabilities, power, and resources constraints, etc.) and diverse services (end-to-end, real-time, QoS, etc.). This situation has put a challenge for the researchers to engineer systems and architectures that will increase the quality of service (QoS) and robustness of the current and future home networks whilst alleviating the management cost and operational complexity.

The characteristics outlined above require some kind of autonomy and intelligent behaviors in the home network. There is an ultimate objective to make the home network as self-behavior network. This leads to the implication of minimum human perception and intervention. All with keeping the network works in an optimal way. This essentially means for a system to be able to self-control and self-manage its internal functions and operations. The network configuration must occur automatically, as well as dynamically adjust to the current configuration to best handle change in the environment. Such configuration makes the network detect failures, faults, and breakdowns in its entities.

To fulfil these requirements, a visionary approach is to build the home network according to the autonomic communication paradigm [1]. Autonomic systems have a range of advantages: they are, for example, cost-effective, robust, fault-tolerant, flexible, scalable, self-configuring, self-healing, and self-managing.

In order to incorporate the autonomic network concepts in the design of network, we first establish a topology based on mesh network for our home network. The mesh topology is the best topology that can fit with the home network due to the distributed and different devices that should communicate directly without the intervention of the base station of regulating their communications. Such communication framework needs a routing protocol based mainly on the QoS metrics. However, routing communication based on conventional protocols can not cope with an environment like home network, since all protocols ranging from physical to application layers need to be improved or reinvented, and the cross layer design among these protocols needed in order to reach the optimal performance. This is our principal motivation to introduce a cross-layer scheme for the design of a communication protocol based on QoS metrics. Such cross-layer design is combined with a knowledge plane in order to enrich the vision of each device in the home network

with all information gathered by this plane. Accordingly, an intelligent decision will be made to select network paths that have sufficient resources to satisfy the QoS requirements of the admitted connections.

The article's organization is as follows. In Section 2, we describe the autonomic mechanisms adopted in our proposal. In Section 3, an analysis of routing metrics in mesh networks is presented. In Section 4, we introduce a QoS-aware routing protocol for mesh networks in future home networks. Simulation results are finally presented in Section 5. Eventually, Section 6 ends the article with our conclusions and future works.

2. AUTONOMIC MECHANISMS

Since home networks' users needs are becoming increasingly various, demanding, and customized, telecommunication networks have to evolve in order to satisfy these requirements. Therefore, a home network has to integrate reliability, quality of service, mobility, dynamicity, service adaptation, and so forth. This evolution will make users satisfied, but it will surely create more complexity in the network generating difficulties in the control process. The motivation behind our choice of autonomic networking inside the home is to hide complexity to home users while using appropriate solutions based on current state/context/content, and on specified policies.

Autonomic communication is the vision of next-generation networking which will be a self-behaving system with properties such as self-healing, self-protection, self-configuration, and self-optimization. Such properties depend on acquiring and understanding the current context of the system. The tasks performed by a device determine the type of information needed. Furthermore, if the context changes, then the system can determine what new data is needed. This requires implementing new distributed functionalities through a novel system architecture to ensure that the networks, as well as home devices and applications, can be deployed and managed, in real-time. To achieve the autonomic-oriented architecture, we propose the following.

(i) Add a distributed knowledge database in the network through the knowledge plane (Section 2.1).

(ii) Organize the home devices according to a mesh topology (Section 2.2).

(iii) And finally add QoS through a smart routing protocol (Section 2.3).

2.1. *The knowledge plane*

In order to realize this vision of autonomic home networks, we must decide how network management is performed. To this end, we have introduced an additional plane (knowledge plane) to the conceptual planes of telecommunication networks (data, control, and management). This yields the model in Figure 1. The data plane or user plane is the part of the network that carries users' traffic, while the control plane is the part of the network that carries control information

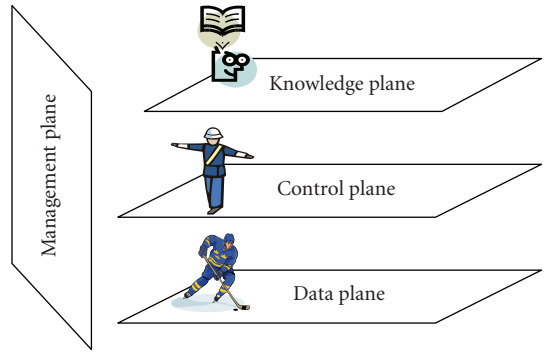

Figure 1: Autonomic architecture.

(also known as signaling), and finally, the management plane carries the operations and administration traffic required to administrate the three other planes.

For implementing any self-function, the system must first be able to *know itself*. One approach to provide this self-knowledge is through the knowledge plane. This new plane should gather, compute, exchange, and provide the network elements all of the knowledge they could need (connectivity, bandwidth, interface load, etc.). It is proposed to encapsulate all layers' independent information as well as the network-wide global view, which can be accessed by all the layers as needed. For modularity, it maintains two entities responsible for maintaining the local and global view. One entity is responsible for the organization of locally available information from different layers in the local network stack and the other data management entity establishes a network wide or global view. The network nodes should constantly update their knowledge plane, as well as exploit it in the decision making.

The sharing of the knowledge does not need to be global. On the contrary, situated knowledge (sharing among a group of neighbours) is enough. Each node builds a primitive situated view of its environment at local scale by gathering information from its protocol layers. Then, exchanging small control messages with its nearest neighbours, the node begins to extend this view.

3. MESH TOPOLOGY

Wireless mesh networks (WMNs) are self-configuring and self-organizing networks, which makes them very suitable option for autonomic home networks. We thus propose to base our architecture on a multihop WMN topology [2].

The wireless mesh network will provide many capabilities for a number of reasons. First, the WMN helps to eliminate dead spots and areas of low-quality wireless coverage throughout the home. Second, due to its powerful communication ability, it facilitates easy information exchange. Third, it enables the network to be set up easily. Finally, deployment cost will be significantly reduced by home mesh routers. These properties make multihop wireless mesh networks very attractive for deployment at home.

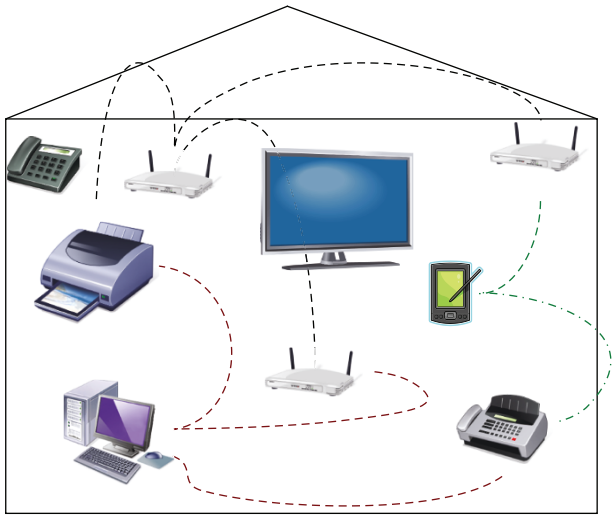

Figure 2: WMN for autonomic home networks.

The wireless mesh home network architecture consists of two categories of physical devices (see Figure 2). The first is called wireless mesh backhauls which are comprised of two types of devices: home mesh access points (MeshAPs) and home mesh routers (MeshRTs). MeshAPs and MeshRTs integrate heterogeneous networks within the home, including, but not limited to, Ethernet LANs, 802.15 WPANs, and 802.11 WLANs, and can be connected to the Internet with gateway functionality. The other category of devices is home meshed clients (MeshCLs). A MeshCL can connect with each other, and connect to the Internet through one or more home mesh routers.

4. QUALITY OF SERVICE SUPPORT

We envision that future home networks will be able to provide highly distributed, pervasive services in a fully autonomic way. Traffics generated by the variety of home applications, ranging from Internet browsing, data backup, and telephony, to entertainment and gaming will have different requirements. The home communication system should be able to get the best of the network infrastructure and resources upon which services operate, being able to ensure sufficient quality of service adaptively and independently of the actual network characteristics (e.g., independently of the fact that we require them from a Wi-Fi PDA, a broadband over power lines TV, or from whatever connectivity and connected devices will be available at that time) [3].

Thus, a key mechanism in autonomic home network services is how to manage the traffic and provide quality of service between the Internet and home networks on one hand, and within diverse home devices on the other hand. Since currently there is no routing protocol that gives optimal performance whatever the network conditions are, we argue that an adaptive and dynamic selection of routing path, taking into account the current traffic situation, is able to optimize the network resources and to come up with a more important number of user expectations associated with QoS.

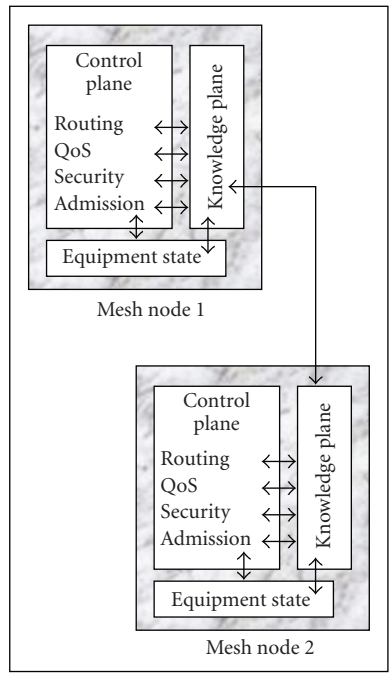

Figure 3: Architecture overview.

To realize such functionalities, it is necessary to be able to configure automatically the network in real-time. To achieve the autonomic-oriented architecture, we propose an optimized QoS-aware routing protocol over the mesh topology which interacts with the knowledge plane to better fit the traffic nature and volume, and the user profiles (see Figure 3).

5. ROUTING METRICS IN WIRELESS MESH NETWORKS

Selecting a good path is considerably harder in wireless networks than in traditional wired networks (where the routing problem is usually solved by running a distributed shortest-path algorithm on a graph) because the notion of a "link" between nodes is not well defined. The properties of the radio channel between any pair of nodes vary with time, and radio communication range is often unpredictable. The communication quality of a radio channel depends on background noise, obstacles, and channel fading, as well as on other transmissions occurring simultaneously in the network.

To ensure good performance, routing metrics must satisfy four requirements. First, the routing metrics must not cause frequent route changes to ensure the stability of the network. Second, the routing metrics must capture the characteristics of networks to ensure that minimum weight paths have good performance. Third, the routing metrics must ensure that minimum weight paths can be found by efficient algorithms with polynomial complexity. Finally, the routing metrics must ensure that forwarding loops are not formed by routing protocols.

There are some promising approaches for improving routing in wireless mesh networks. They are mainly based

on adapting some well-known ad hoc routing protocols such as AODV [4], DSR [5], or OLSR [6]. In this section, we will analyze the performance of four existing routing metrics for ad hoc networks: RTT [7], ETX [8], ETT [9], and WCETT [10].

5.1. Per-hop round trip time (RTT)

This metric is based on measuring the round trip delay seen by unicast probes between neighboring nodes. To calculate RTT, a node sends a probe packet carrying a timestamp to each of its neighbors every 500 milliseconds. Each neighbor immediately responds to the probe with a probe acknowledgment, echoing the timestamp. The RTT metric is designed to avoid highly loaded or lossy links. Since RTT is a load-dependent metric, it can lead to route instability. Moreover, this measurement technique requires that every pair of neighboring nodes probes each other. Thus, the technique might not scale to dense networks.

5.2. Expected transmission count (ETX)

ETX is defined as the expected number of MAC layer transmissions that is needed for successfully delivering a packet through a wireless link. The weight of a path is the summation of the ETX's of all links along the path. Since both long paths and lossy paths have large weights under ETX, the ETX metric captures the effects of both packet loss ratios and path length. In addition, ETX guarantees easy calculation of minimum weight paths and loop-free routing under all routing protocols. However, the drawbacks of ETX are that it does not consider interference or the fact that different links may have different transmission rates.

5.3. Expected transmission time (ETT)

The ETT routing metric improves ETX by considering the differences in link transmission rates. The ETT of link l is defined as the expected MAC layer duration for a successful transmission of a packet at link l. The weight of a path p is simply the summation of the ETTs of the links on the path. The relationship between the ETT of link l and ETX can be expressed as follows:

$$\mathrm{ETT}_l = \mathrm{ETX}_l \; s/b_l, \tag{1}$$

where b_l is the transmission rate of link l and s is the packet size. Essentially, by introducing b_l into the weight of a path, the ETT metric captures the impact of link capacity on the performance of the path. However, the remaining drawback of ETT is that it still does not fully capture the intraflow and interflow interference in the network.

AODV-ST [4] is another protocol that uses estimated transmission time (ETT) as the routing metrics. Mesh routers make a spanning tree corresponding to each gateway in the network. A load balancing technique is used to route the traffic to the least loaded gateway.

5.4. Weighted cumulative ETT (WCETT)

In WMNs, multiradio per node may be a preferred architecture, because the capacity can be increased without modifying the MAC protocol. A routing protocol named (MR-LQSR) is proposed in [11] for multiradio WMNs. A new performance metric, called the weighted cumulative expected transmission time (WCETT), is proposed for the routing protocol. WCETT takes into account both link quality metric (losses, bandwidth, ...) and the minimum hop-count. It can achieve good trade-off between delay and throughput because it considers channels with good quality and channel diversity in the same routing protocol.

6. THE QOS-AWARE MESH ROUTING PROTOCOL "SAM"

Despite the availability of several routing protocols for ad hoc networks, the design of routing protocols for WMNs is still an active research area. In [12], it was shown that finding the optimal route in a multiradio wireless mesh networks is NP-hard problem. New performance metrics need to be discovered and utilized to improve the performance of routing protocols. Moreover, the existing routing protocols treat the underlying MAC protocol as a transparent layer. However, the cross-layer interaction must be considered to improve the performance of the routing protocols in WMNs. More importantly, the requirements on power efficiency and mobility are much different between WMNs and ad hoc networks. In a WMN, nodes (mesh routers) in the backbone have minimal mobility and no constraint on power consumption, while mesh client nodes usually desire the support of mobility and a power efficient routing protocol.

Such differences imply that the routing protocols designed for ad hoc networks may not be appropriate for WMNs. Based on the performance of the existing routing protocols for ad hoc networks and the specific requirements of WMNs, we believe that an optimal routing protocol for WMNs must capture the following features.

(i) Performance metrics: many existing routing protocols use minimum hop-count as a performance metric to select the routing path. This has been demonstrated not to be valid in many situations. To solve this problem, performance metrics related to link quality are needed. If congestion occurs, then the minimum hop-count will not be an accurate performance metric either. Usually round-trip time (RTT) is used as an additional performance metric. The bottom line is that a routing path must be selected by considering multiple QoS performance metrics such as energy consumption.

(ii) Fault tolerance with link failures: one of the objectives to deploy WMNs is to ensure robustness in link failures. If a link breaks, the routing protocol should be able to quickly select another path to avoid service disruption.

(iii) Load balancing: one of the objectives of WMNs is to share the network resources among many users. When a part of a WMN experiences congestion, new traffic flows should not be routed through that part. Performance metrics such as RTT help to achieve load balancing, but are not always effective, because RTT may be impacted by link quality.

Based on these observations, we propose a Qo**S**-**a**ware routing **m**esh (SAM) protocol. The goal of SAM is to build a wireless mesh network routing protocol that provides QoS guarantees to applications inside the home. This means that the service level and the network level cannot work as separated universe, each towards its own goals. Rather, the routes discovered by our routing protocol will feet to application requests for desired bandwidth and delay bounds for the flow, or deliver an end-to-end flow that satisfies those performance bounds at the time of the request. If the route is disrupted by node or link failure, the protocol automatically detects the route breakages, and rediscovers alternate routes if they exist. SAM is a reactive protocol that discovers routes on demand.

Cross-layer design between routing and Medium Access Control (MAC) protocols is another important characteristic in SAM. Previously, routing protocol research was focused on layer-3 functionality only. However, adopting multiple performance metrics from layer-2 into routing protocols such as power consumption and link security level is a promising approach. In fact, we are observing an increasing number of network technologies with heterogeneous properties. Some of today's networking technologies—specially those tied to fixed infrastructure, like cables—will exist for some time. At the same time, new technologies emerge which may be not only low power-consuming wireless networks with low bandwidth (e.g., Bluetooth), but also high-speed wireless networks (WiFi, WiMax, etc.) as well as very high-speed optical networks. Not only will the bandwidth differ in these networks, but also their reliability, like bit error rate. SAM protocol will exploit such information in the decision making. This can be done through the interaction with the knowledge plane. Having a great amount of data, the knowledge plane correlates them to provide more significant, and then useful information.

6.1. Service classes and QoS algorithm

The objective of SAM is selecting network paths that have sufficient resources to satisfy the QoS requirements of the admitted connections. Many paths between the source and the destination may be available. Because there is no available centralized controller that knows the whole picture of the network resources, SAM calculates link weights hop by hop, and then combines them into a path metric. SAM is a source-routed protocol derived from AODV protocol. Route discovery and metric calculation are based on route request and route response mechanisms.

6.1.1. Assumptions

We begin by listing some assumptions we made about the home network in which SAM is supposed to operate. These assumptions are not necessary for the correct operation of our protocol; they only simplify the case study.

First, we suppose that the home network is only composed of three technologies: WiFi, Bluetooth, and Ethernet. To measure path performances, we have defined five metrics: (1) available bandwidth, (2) end-to-end delay, (3) WCETT, (4) security level, and (5) energy consumption level. These metrics translate application requirements (in terms of bandwidth, transaction security, and tolerated delay) and networks needs (in terms of congestion, loss rate, and consumed energy).

We assume that each service flow will provide the following QoS parameters to the knowledge plane: the minimum required bandwidth $B_{\min}$, the maximum tolerated end-to-end delay from the source to the destination $T_{\max}$, and the minimum required security level S_{level}. Instead of the shortest-path algorithm, SAM uses a combination of WCETT, available bandwidth B_{avai}, end-to-end delay $T_{\max}$, link energy E_i, and link security level S_i as metrics.

Each node can get its available bandwidth B_{avai} and WCETT_i on the current link i by simply asking the knowledge plane (see Figure 4).

6.1.2. Route selection algorithm

Our routing algorithm is implemented in the following four steps on-demand hop-by-hop route discovery procedure.

Step 1 (Route discovery). When a source node S originates new flow addressed to node D, it checks if it has a fresh route from S to D that satisfies QoS requirements of the application A that originates the flow. We get the QoS requirements of A from the knowledge plane. If such route exists (this is scarcely the case), we use it. If no route to D satisfies QoS requirements of the running application A, Sbroadcasts a route request packet (RREQ). Nodes along possible routes are explored by the route request packets from the source. These packets travel through each node along the candidate routes to obtain bandwidth availability, link energy E_i, and link security level S_i as well as gather the end-to-end delay information of the route.

Each node that receives the RREQ packet checks first if it is the solicited node. If this is the case, then it sends a route reply packet (RREP). Else, it updates network QoS parameters on the RREQ message before it forwards it to the destination. This is done in the following manner

$$\begin{aligned} \text{Security} &= \min(\text{Security}, \text{local } S_i), \\ \text{Energy} &= \text{Energy} + \text{local } E_i, \\ \text{Delay} &= \text{Delay} + \text{local } D_i, \\ \text{Bandwidth} &= \min(\text{Bandwidth}, \text{local } B_{\text{avai}}). \end{aligned} \tag{2}$$

Finally, we obtain at the destination D the following metrics for a particular path j from S to D

$$\begin{aligned} \text{Security}(j) &= \min(S_i), \\ \text{Energy}(j) &= \text{sum}(E_i), \\ \text{Delay}(j) &= \text{sum}(D_i), \\ \text{Bandwidth}(j) &= \min(B_{\text{avai}}), \\ E(j) &= \text{Energy}(j)/\text{number of hops}. \end{aligned} \tag{3}$$

Step 2 (Route selection). Route selection is done at the destination node D to limit network flooding with route reply messages.

Table 1: Applications' QoS requirements.

Traffic type	BW	Loss rate	Delay	Jitter
Voice	Low	Medium	High	High
E-commerce	Low	High	High	Low
Transaction	Low	High	High	Low
Email	Low	High	Low	Low
Telnet	Low	High	Medium	Low
Browsing	Medium	High	High	Low
File transfer	High	Medium	Low	Low
Video conferencing	High	Medium	High	High
PnP control message	Low	High	Medium	Low

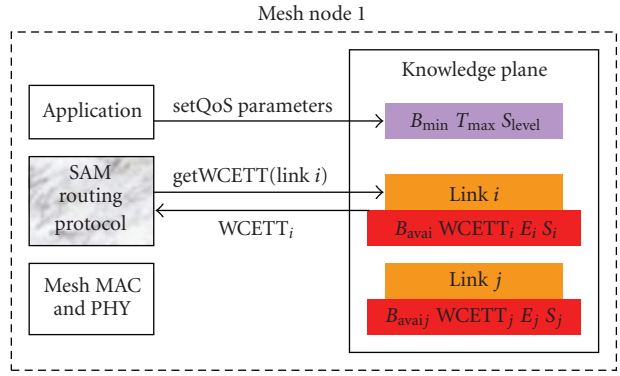

Figure 4: SAM conceptual architecture.

■ *Case: application = voice*
$P = \{\text{Paths/delay} \le T_{max} \& \text{Security } S \ge S_{level}\}_{\min E}$
■ *Case: application = client/server(email, telnet ...)*
$P = \{\text{Paths}/S \ge S_{level}\}_{\min (\text{WCETT}, E)}$
■ *Case: application = file transfer*
$\text{Path} = \{\text{Paths}/B_{avai} \ge B_{min} \text{ and } S \ge S_{level}\}_{\min E}$
■ *Case: application = video conferencing, multicasting*
$P = \{\text{Paths}/B_{avai} \ge B_{min} \text{ and } S \ge S_{level}\}_{\min(\text{WCETT},E)}$

Algorithm 1: Selection algorithm.

Normally, the destination node will receive several RREP packets through different paths with different characteristics (metrics values). It has to choose the best one according to the current application QoS requirements. Table 1 shows QoS requirements of some well-known applications.

We denote P as the selected path. We classify applications into four main classes.

(i) Class 1: composed of applications that are exigent on delay such as voice.

(ii) Class 2: composed of applications that are exigent on delay and loss rate such as e-commerce, email, and control messages (UPnP). We use WCETT to aggregate these two metrics.

(iii) Class 3: composed of applications that are exigent on bandwidth such as file transfer.

(iv) Class 4: composed of applications that are exigent on bandwidth, loss rate and delay such as video conferencing applications. We use WCETT to aggregate these 3 metrics.

The destination node D will execute a pseudoalgorithm reported on Algorithm 1 to choose the appropriate path.

For example, for voice the selected route will be the path that minimizes energy while having an end-to-end delay less or equal to the maximum tolerated application delay T_{max} and a security level superior or equal to the S_{level} required by the application. For an application type client/server, the algorithm selects the path from those with a security level superior or equal to the S_{level} that minimizes WCETT and energy consumption.

Step 3 (Route registration). Bandwidth B_{min} is registered at each node along the reverse routes explored, by the route reply packets from the destination. This mechanism allows intermediate nodes to set up their routing tables and to reserve the correct bandwidth to (source address and destination address) duplet.

Step 4 (Route activation). The route is activated by the data transmission of the actual traffic flow, and bandwidth reservation will take effect.

The choice of radio technology influences the performance of the network and thus the routing protocol needs to be aware of it, and cannot operate in the same way as wired networks which are agnostic about the underlying medium. For better path selection process, we introduce technologies specificities and preferences in the routing algorithm through the value that we attribute to the link energy consumption parameter E_i and link security level parameter S_i. For example, S_i is high for an Ethernet link and low for an insecure WiFi link. Respectively, E_i is high for wireless connections and low for an Ethernet link.

7. PERFORMANCE RESULTS

In order to evaluate our solution, we started by implementing SAM on the NS-2 network simulator. The most important task is on the implementation of the knowledge plane. We have created a dedicated class which gives us the different network metrics values. These metrics are dynamics and can change during the simulation time. As for the applications metrics, we give these metrics values to the class statically at the beginning of the simulation.

7.1. Scenarios

We have studied two scenarios. Both are based on the network topology plotted on Figure 5. Mainly two types of traffic sources are used (FTP and voice) as in [13]. The FTP traffic requires more bandwidth than voice traffic as it can be

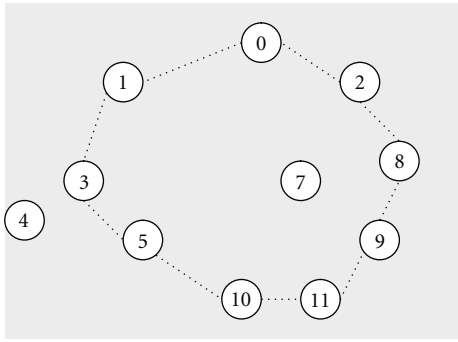

Figure 5: Network simulation topology.

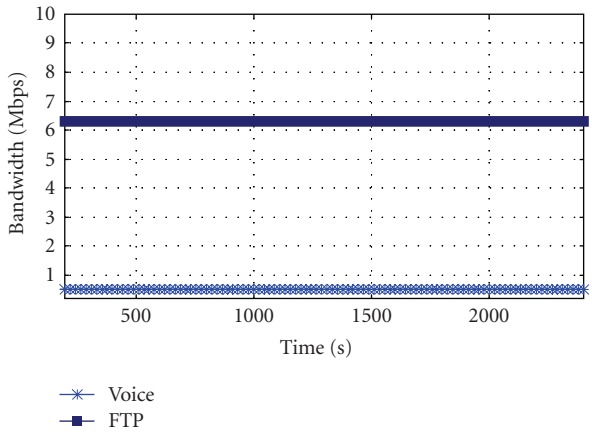

Figure 6: FTP and voice flows under SAM.

Table 2: Scenario 1 parameters.

Parameter	Value
Transmission range	10 m
Source address	5
Destination address	9
Number of flows	2
Flow1 application class	FTP
Flow2 application class	Voice
Flow1 packet size	1024 B
Flow2 packet size	128 B

Table 3: Scenario 2 energy parameters.

Node	Initial energy	Transmission power
0	99	0.02
1	100	0.05
2	98	0.09
3	96	0.02
4	96	0.02
5	96	0.02
6	96	0.02
7	97	0.04
8	95	0.07
9	96	0.02
10	102	1
11	104	1.1

seen in Table 2. However the voice flow is more sensible to delay.

In the first scenario, an attempt was made to compare SAM performance to the basic AODV standard under the same application flow. This is achieved by comparing performance of AODV and SAM using two flows types with different QoS metrics: FTP and voice. Table 2 shows the first scenario parameters. We set all links bandwidth to 11 MB except those that are to or from node 11 which are set to 2 MB. The energy consumption level is equal in all nodes. These two flows start simultaneously at 10 seconds from the same source node 5 to the same destination node 9.

The second scenario aim is to show that SAM takes also into account energy consumption per path. Note that optimizing this value increases the lifespan of network nodes. To achieve this, we initiate an FTP flow from node 5 to node 9. Bandwidth is set to 11 MB on all links. We add different energy capabilities to network nodes. Table 3 shows the energy parameters of each node.

7.2. Bandwidth and delay impacts

In the first scenario, SAM selects the path 5-3-1-0-2-8-9 for the FTP flow and the path 5-10-11-9 for the voice. This means that SAM has selected different paths based on each application requirements; one with higher bandwidth for the FTP traffic (because node 11 has a limited bandwidth of only 2 MB) and one with minimum delay for voice. However, AODV selects the same path for the two flows 5-10-11-9 because it computes routing paths based on the shortest path algorithm with no further QoS consideration.

Figures 6 and 7 show that SAM outperforms AODV under the two types of applications flows. For the same FTP flow, SAM offers 6.3 Mbps whereas AODV offers only 3.9 Mbps. Figure 8 confirms that SAM offers a differentiated routing service per application type. The average end-to-end delay of packet delivery was higher in FTP compared to the voice flow, whereas AODV offers the same end-to-end delay because the two flows use the same path. It is noticeable that SAM is more adapted to real-time applications.

7.3. Energy consumption

In the second scenario, since we have used FTP flow and the same bandwidth on each link, SAM will choose a path which minimizes the energy consumption per node. Whereas, AODV still chooses the shortest path, even if this path consumes more energy.

SAM chooses the path 5-3-1-0-2-8-9 (because node 11 and 10 consume a lot of energy) while ADOV uses the same path as in first experience that is, 5-10-11-9. Figure 9 plots energy consumption of some nodes in the SAM path and some nodes of AODV selected path. We can clearly see that the path selected by the SAM protocol will consume less

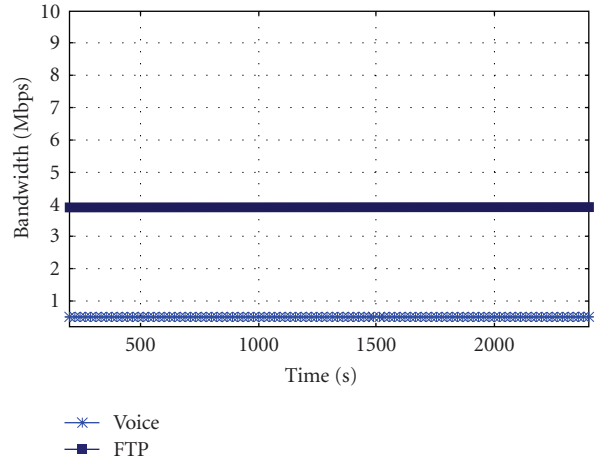

Figure 7: FTP and voice flows under AODV.

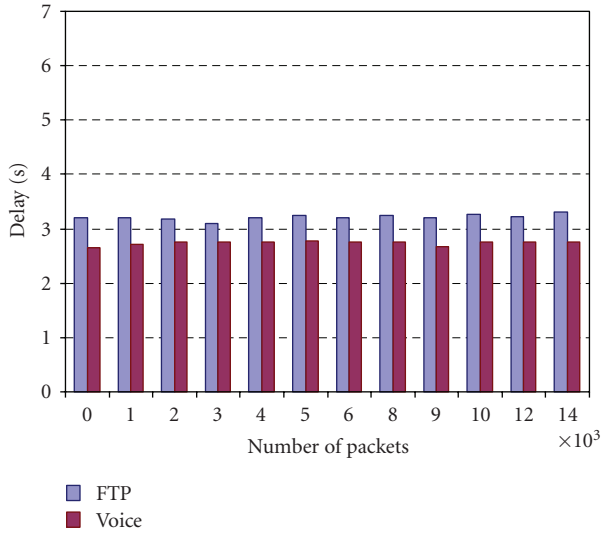

Figure 8: End-to-end delay for FTP versus voice under SAM.

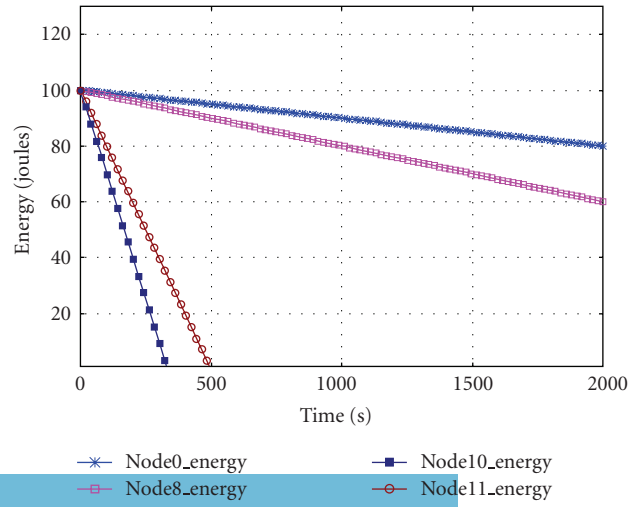

Figure 9: Energy consumption in scenario 2.

energy and is then more robust against nodes dead. However, in the AODV path, the node 11 breaks down rapidly after approximately 300 seconds because the AODV standard does not take into consideration such parameter in the route selection process.

8. CONCLUSION

The capability of self-organizing in WMNs reduces the complexity of network deployment and maintenance, and thus, requires minimal upfront investment. Such self-organizing is one of the concepts go that the autonomic networking. Based on such concept, a new QoS-aware architecture for autonomic home networks has been presented and evaluated. Our proposal is based on introducing the knowledge plane to the conceptual planes of network framework. The incorporation of the knowledge plane over the network allows to obtain more accurate information of the current and future network states which helps the routing protocol in the decision-making process. Our goal is to maintain a stable route which provides per flow guarantee quality of service while taking advantage of heterogeneous link layer characteristics. We have shown through simulations the viability of our proposal. In our future work, we intend to analyze the capacity of WMNs as all theoretical results on the capacity of WMNs are still based on some simplified assumptions. We will investigate the performance of our autonomic approach in order to calculate the WMNs capacity and comparing it with the conventional methods of capacity calculation.

REFERENCES

[1] S. Schmid, M. Sifalakis, and D. Hutchison, "Towards autonomic networks," in *Proceedings of the 1st International IFIP TC6 Conference on Autonomic Networking (AN '06)*, pp. 1–11, Paris, France, September 2006.

[2] I. F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: a survey," *Computer Networks*, vol. 47, no. 4, pp. 445–487, 2005.

[3] F. Licandro and G. Schembra, "Wireless mesh networks to support video surveillance: architecture, protocol, and implementation issues," *EURASIP Journal on Wireless Communications and Networking*, vol. 2007, Article ID 31976, 13 pages, 2007.

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

[5] D. B. Johnson, D. A. Maltz, Y. Hu, and J. G. Jetcheva, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)," IETF Internet Draft, February 2002.

[6] T. Clausen and P. Jacquet, "Optimized Link State Routing Protocol (OLSR)," RFC 3626.

[7] A. Woo, T. Tong, and D. Culler, "Taming the underlying challenges of reliable multihop routing in sensor networks," in *Proceedings of the 1st International Conference on Embedded Networked Sensor Systems (SenSys '03)*, pp. 14–27, Los Angeles, Calif, USA, November 2003.

[8] R. Draves, J. Padhye, and B. Zill, "Comparison of routing metrics for static multi-hop wireless networks," in *Proceedings of the ACM Conference on Applications, Technologies,*

Architectures, and Protocols for Computer Communications (SIGCOMM '04), pp. 133–144, Portland, Ore, USA, August-September 2004.

[9] D. S. J. De Couto, D. Aguayo, J. Bicket, and R. Morris, "A high-throughput path metric for multi-hop wireless routing," in *Proceedings of the 9th Annual International Conference on Mobile Computing and Networking (MobiCom '03)*, pp. 134–146, San Diego, Calif, USA, September 2003.

[10] R. Draves, J. Padhye, and B. Zill, "Routing in multi-radio, multi-hop wireless mesh networks," in *Proceedings of the 10th Annual International Conference on Mobile Computing and Networking (MobiCom '04)*, pp. 114–128, Philadelphia, Pa, USA, September-October 2004.

[11] K. Ramachandran, M. Buddhikot, G. Chandranmenon, S. Miller, E. Belding-Royer, and K. Almeroth, "On the design and implementation of infrastructure mesh networks," in *Proceedings of the 1st IEEE Workshop on Wireless Mesh Networks (WiMesh '05)*, pp. 4–15, Santa Clara, Calif, USA, September 2005.

[12] M. Alicherry, R. Bhatia, and L. Li, "Joint channel assignment and routing for throughput optimization in multi-radio wireless mesh networks," in *Proceedings of the 11th Annual International Conference on Mobile Computing and Networking (MobiCom '05)*, pp. 58–72, Cologne, Germany, August-September 2005.

[13] L. Iannone, K. Kabassanov, and S. Fdida, "Evaluation of cross-layer rate-aware routing in a wireless mesh network test bed," *EURASIP Journal on Wireless Communications and Networking*, vol. 2007, Article ID 86510, 10 pages, 2007.