Towards Control Message Quenching for SDWSN: A State of the Art Overview

Musa Ndiaye*, Gerhard P. Hancke*, Adnan M. Abu-Mahfouz*†
*Department of Electrical, Electronic and Computer Engineering, University of Pretoria, Pretoria
[1]mndiaye@ieee.org
[2]gerhard.hancke@up.ac.za
†Council for Scientific and Industrial Research (CSIR), Pretoria
[3]a.abumahfouz@ieee.org

***Abstract*—The deployment of wireless sensor networks (WSNs) has rapidly expanded with the widespread implementation of the internet of things (IoT) technologies. However, traditional WSNs are resource-constrained and offer rigidity in network management especially with wide-scale implementation. Software-defined networking (SDN) based on the provision of a centralised controller promises to improve flexibility and ease of managing large scale WSNs. This has been made possible through the separation of the control intelligence from the data forwarding infrastructure of network devices. However, SDN-based implementation comes at a cost of control overhead traffic which is a performance bottleneck to WSNs due to the limited in-band traffic channel bandwidth associated with WSNs. This has driven the research community to look into methods of effectively reducing the overhead control traffic in a process known as control message quenching (CMQ). This paper provides a state of the art overview of control traffic reduction techniques available and being implemented for SDN-based WSNs. It provides an insight of benefits, challenges and open research areas available in the field of control message quenching in SDN-based WSN. This paper opens the door to this widely unexplored research area in its current form.**

***Index Terms*—Wireless sensor network, software-defined networking, control message quenching, overhead traffic.**

I. Introduction

The internet of things (IoT) has brought with it several applications in industry and society at large [1]. We are seeing more implementation on a much larger scale for smart city development [2] and also in the medical industry for targeted health needs. The direct impact of this is the deployment wireless sensor networks (WSN) to the scale of hundreds of thousands of sensor nodes in varying environments which include harsh and hard to reach areas. Most of these sensor nodes are provided by different vendors and hence resulting in a heterogeneous setup that creates a management challenge especially with remote node reprogramming and general vertical application integration [3]. This management complexity is further magnified with large scale WSN implementations and the resource-constrained nature of WSN. Software-defined networking (SDN), a paradigm based on providing global control of networks by separating the network intelligence from the data infrastructure (switches, nodes) promises the efficiency of flexible management in tacking the above said WSN management problem. The resulting resource-capable and logically centralized controller maintains a global view of the entire network allowing ease of policy implementation and network reprogramming regardless of network heterogeneity [4].

However, the operating principle of SDN-based WSNs (SDWSN) is based on the provision of flow rules and other related traffic (control traffic) to and from the data infrastructure in the data plane which in the case of WSN implementation has to occupy the same in-band traffic channel with data plane traffic [5], [6]. This unlike in computer networks where a dedicated out-band control channel can be provisioned and thus overhead control traffic is a potential bottleneck to packet delivery, latency and controller responsiveness in SDWSN. In this regard, there has been a general interest in the SDWSN research industry to effectively reduce the levels of overhead control traffic also referred to as control message quenching (CMQ) [7].

This paper aims to provide an overview of CMQ techniques in SDN-based WSNs and is organised as follows: Section II provides general background on the need for overhead control traffic reduction including efforts in the computer network based SDN while Section III provides an in-depth overview of CMQ techniques available for SDN-based WSNs and attempts to categorise them accordingly. Section IV tries to identify the relationships that may exist between control message reduction and network performance metrics in a bid to avoid quality of service (QoS) compromise in the process. Section V identifies future open research areas in the field of CMQ for SDN-based WSNs and finally in Section VI, we draw conclusions and discuss some lessons learnt based on the findings.

II. Background

The SDN implementation in WSN enables global control of network devices via a set of control policies handled by the southbound application protocol interface (API) between the control plane and the data plane. The control policies are categorised into packet types based on function. Fig. 1 shows the architecture of this SDN-based operation in WSNs.

The various control traffic packet types can be categorised as:

(a) Flow setup: This type of traffic flows from the control plane to the data plane and is composed of flow rules required for routing in the data plane. A flow setup packet

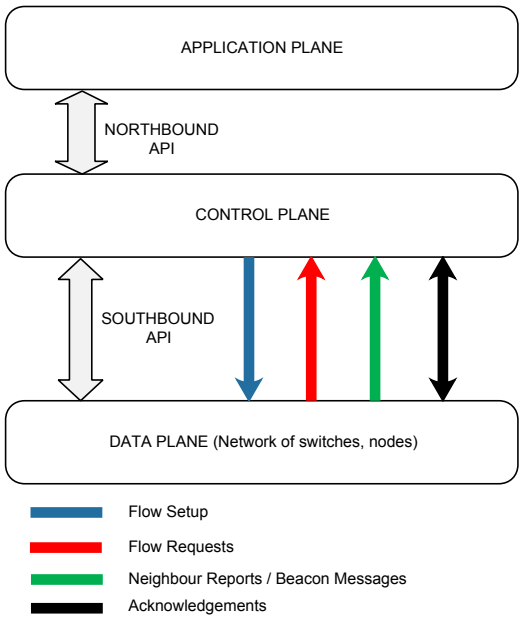

Fig. 1. Control traffic in SDWSN

can be issued at bootstrapping or in response to a flow request.

(b) Flow requests: In a typical Sensor OpenFlow (SOF) setup [5], when a packet arrives at an SDN-enabled sensor node, the packet source address or flow ID is cross-checked with the flow table rules in the SDN-enabled node. If a match is found, the packet is processed according to the routing actions in the table but if a mismatch occurs a flow request packet is issued to the controller to send an associated flow setup.

(c) Neighbour reports / Beacon Messages: Routing requires up to date localisation of sensor nodes in the data plane and regular neighbour reports or beacon messages are required to obtain a good estimate of node locations. A neighbour report contains information such as neighbour address and estimated transmission count (ETX). The frequency of this kind of control packet is dependant on the underlying neighbour discovery protocol implemented in the SDN-based WSN.

(d) Acknowledgements: This control packet type can be used to confirm the successful delivery of a policy or data packet. Depending on the design requirements, the controller or node may require an acknowledgement packet as part of the network management policy and control.

While control traffic plays an important role in enabling the management flexibility that SDN provides, overhead control traffic has been identified as a drawback in obtaining the desired QoS. In TinySDN [6] authors mention that increased in-band control traffic places a limit on the data transmission rate potentially leading to increased packet delay. Bera et al. [8] find in their implementation of an SDN-based WSN that the control traffic generated is higher than in traditional WSNs. As part of the authors' conclusion, they propose further work be done in minimizing the resulting control message overhead. Lasso et al. [9] also found the need to further examine network control message reduction as part of their implementation of an SDN-based IoT framework for IPV6 over low-power wireless personal area networks (6LoWPAN).

In computer network-based SDN, control message quenching has mainly been adopted to increase controller responsiveness not so much for bandwidth requirements due to the possibility of providing a dedicated control channel. Popular solutions for CMQ in such networks involve use of multiple controllers to share the control traffic load and hence improve controller responsiveness. Contributions such as DevoFlow [10] and that by Yu et al. [11] are based on this approach. One of the early adopters to implement a CMQ method that is simple and does not require modification of the control plane include Luo et al. [7]. They use a reference memory to prevent the generation of duplicate flow request packets and notice improved controller responsiveness upon implementation. Others such as Obadia et al. [12] use a greedy heuristic algorithm that calculates the cost of control traffic based on awake nodes and available controllers.

III. Control Message Quenching for SDN-based WSNs

To open a discussion on minimization techniques for control traffic in SDN-based WSNs, we identify the main categories for control message quenching and highlight the contributions therein.

A. *Controller distribution / Traffic load sharing*

The use of distributed controllers in SDN-based applications is becoming increasingly popular as a form of control message quenching. Multiple controller integration allows for sharing of the overall traffic load and depending on the implementation can significantly improve controller responsiveness and reduce packet latency. Reliability is another direct advantage of this approach as distributed control would still result in service continuity even during the downtime of some of the controllers in the network which would not be the case with a single centralized controller [13].

The multiple controllers are usually designed hierarchically with a global controller coordinating and synchronising multiple local controllers which may each be assigned to a cluster of sensor nodes. The global controller plays an active role is giving partial authorisation to the local controllers to perform routing and flow operations locally. There have been implementations of this kind of CMQ in SDWSN literature. Oliveira et al. [6] for example use distributed controllers in their TinySDN implementation to tackle challenges such as communication latency, overhead control traffic and limited energy supply. Issues of controller placement have also been investigated in TinySDN with a noticeable improvement in

performance when the controllers are placed nearer to the end devices (sensor nodes). Galluccio et al. [14] in SDN-WISE provide support for distributed controllers to improve controller response times while highlighting the need for security in the controller software. We observe that the use of multiple controllers in an SDN-based WSN provides a promising solution however it offers challenges in terms of controller synchronisation and also requires redesigning the control plane.

B. Control aggregation/ Fusion

Data aggregation and/or data fusion has been used severally in reducing data traffic both in traditional WSNs and SDWSNs. Techniques such as taking the average value of a measurand like temperature, humidity etc and sending only one average value of a cluster area to the sink instead of multiple readings have been implemented. However, the idea of using this aggregation or data fusion method in reducing control messages in SDN-based WSN is still very niche and limited in terms of application. This form of control message quenching can be approached either by modifying flow-table rules to combined multiple flow instructions into a single flow packet or by simple packet concatenation of packets that are sent along the same paths.

Friedman et al. [15] open a discussion on modification of flow-table rules to enable data aggregation in their proposed SDN-based WSN architecture. Although, in their discussion, a demonstration of fusion of data traffic such as temperature and humidity is given and not specifically control traffic packets. We observe and conclude that the implementation of such a technique for minimizing control traffic may require an algorithm to group common flow-table items and discarding of duplicate data from multiple related flow packets.

In SDN-WISE [14] an early attempt at packet concatenation to minimize control traffic is made as part of the in-network packet processing (INPP) layer. Galluccio et al. use the INPP layer to concatenate small packets being sent along the same route and hence minimizing the overhead. However, it is clear that a need for further network coding to effectively target control traffic minimization in the implementation of SDN-WISE.

The general concept of using data aggregation / fusion to reduce the number of control packets arriving at the controller and as a result improving controller time response is illustrated in Fig. 2.

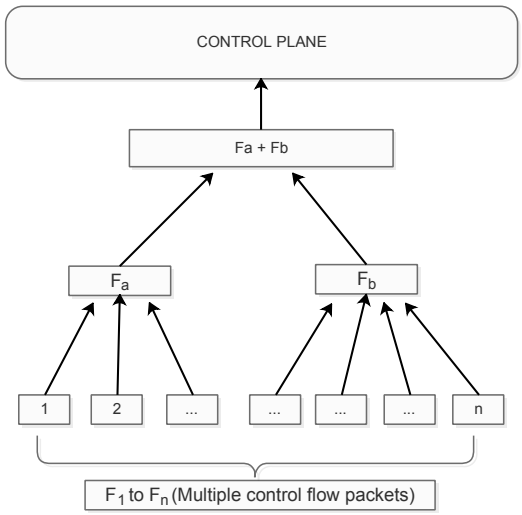

Fig. 2. Control flow aggregation / fusion concept

C. Collect-based approach

A more direct approach to reducing control traffic is based on locally preventing excess collection and transmission of control policies. The collect protocol for neighbour discovery, for example, can be adjusted to send fewer neighbour reports or beacon messages to the controller. Galluccio et al. [14] mention how the frequency of topology discovery packet generation and associated neighbour information report affect the overhead in SDN-WISE. However, it is important to note that adjusting the collect protocol in a bid to reduce overhead affect other network performance parameters and as such, this tradeoff should be taken into account during design and implementation.

Another simpler approach of reducing control messages is by preventing transmission of duplicate control packets which may result from recurrent requests for the message to be sent to the controller. Lu et al. [7] identify a typical scenario where duplicate flow requests are prevented from being generated. Flow requests are generated upon table mismatch and once a similar packet (same source/destination address or flow ID) arrives at a node another flow request of the same type will be generated as long as a flow setup from the initial request has not arrived from the controller to update the node table. A similar case can also occur on the controller side during flow setup and a notable solution to preventing this form of duplication is by using a reference memory that can either be external or internal to the devices. Upon initial flow request, the associated source/ destination address can be stored in dynamic memory list and this list can be referred to thereafter whenever a mismatch occurs. If the source/ destination pair details do not match anything in the list, a flow request is generated otherwise the flow request is suppressed and the packet enqueued waiting to be processed when the original flow setup update arrives. Asaduzzaman et al. [16] recently proposed a similar technique but based on a separate and external memory reference. However, in SDN-based WSN this approach to CMQ remains widely unexplored. Fig. 3 shows the basic implementation setup of this control traffic reduction method.

D. Heuristics/ Cognitive approach

Network intelligence and learning approaches can be used to ensure a minimum and optimal control traffic rate. Cal-

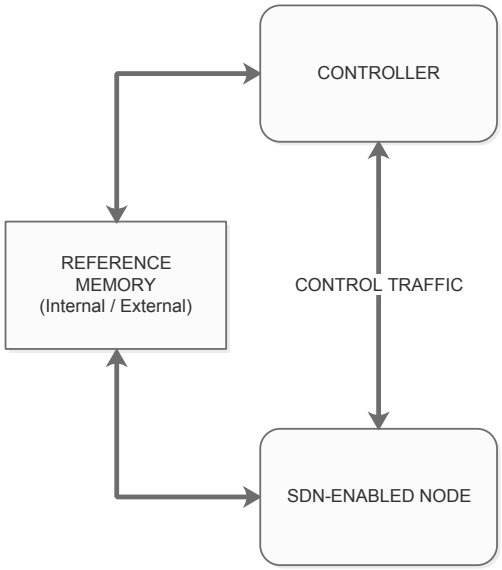

Fig. 3. CMQ based on reference memory

culations performed can ensure that the cost of transmitting control data are not more than what is required based on available and awake devices in the network at that particular time. The feasibility of this mechanism in reducing control traffic has been demonstrated for conventional SDN by Obadia et al. [12]. While network learning and heuristics promise the potential of optimizing control traffic, this technique is still very niche in SDN-based WSNs. Additionally, active-sleep scheduling techniques can further be used to minimize the amount of control traffic operations required in a network to meet the desired QoS at a particular time.

Table I shows a summary of a qualitative comparison of the control message quenching techniques discussed in this section. We compare what modifications to the SDN architecture are required, the complexity of implementation and the current state of the application in the SDWSN field.

TABLE I
COMPARISON SDN-BASED WSN CMQ TECHNIQUES

Method	Modification	Complexity	Application
Distributed controller	Control plane	Medium - High	Common
Control aggregation	Flow table/ flow rules	Medium - High	Limited
Collect	Data or control planes	Low	limited
Heuristics	Variable	Medium - High	Very limited

IV. DESIGN CONSIDERATIONS FOR SDWSN-BASED CMQ

In a bid to reduce control overhead in SDWSNs, it should be taken into consideration that there exists at the trade-off between the level of control traffic minimization and the design requirements of SDN-based WSNs such as packet delivery rate (PDR), latency and energy efficiency. In terms of using distributed controllers to quench control traffic, the implementation should account for the resulting packet delay in using multiple controllers. Techniques to improve synchronization and reduce delay need to be investigated and implemented. Kobo et al. [17] propose the use of fragmentation to reduce the end to end delay in multiple controller setups for SDWSNs.

In scenarios where topology discovery packets such as beacon messages are lowered to reduce overhead, the design requirement should also take into account the complexity of the network topology and how much the network parameters and node locations fluctuate. Rapid variations in network parameters require frequent and up to date topology discovery messages. The level of control traffic minimization should be optimized against the packet delivery rate and delay. Energy efficiency should also be taken into account as poor topology discovery may result in poor and energy inefficient packet routing and link failures.

While aggregation methods may result in improved energy efficiency, the time complexity in implementing the method may lead to packet delay. This is also the same for heuristic methods which involve lots of complex computations.

V. CMQ FUTURE RESEARCH CHALLENGES

Future research requires further investigation into methods of control message quenching involving heuristics and machine learning. There is a need to implement mathematical optimization techniques that increase the design requirement yield based on the trade-off that exists between overhead reduction and the desired QoS in SDWSN. There is a need to implement aggregation or data fusion techniques for control flow traffic with a clear outline of how the flow tables and rules can be modified to achieve this. While researchers have begun proposing more efficient and low latency ways of implementing distributed controllers in SDN-based WSNs there is still a need for more work in this area in terms of synchronization and also security.

The efficiency of flow table rules in the data plane can also further investigated especially the aspect of nodes sharing and synchronizing rules that have already been issued by the controller instead of each node making a request whenever need arises while it is possible that another node in the plane may have the required flow rules at that particular time.

Fallback mechanisms can be investigated to minimize flow setup requests. Possible solutions may include backup packet routing for mismatched packets or achieving node localisation with locally implemented mechanisms. An example of backup packet routing would involve proactively installing rules to reduce the number of flow requests that need to be sent to the controller. These backup rules can also aid routing if a neighbour fails or the controller becomes unresponsive.

VI. Conclusion

In this paper, we have discussed an overview of the current state of control traffic overhead reduction methods for SDN-based WSNs. Having considered the background on the need for control message minimization we highlighted the categories of control message quenching and the available contributions in research and implementations therein. Challenges in reducing control traffic while trying to meet the minimum design requirements have also been discussed and the open research areas available to solve some of the mentioned challenges. We learn a few things from the current state of control traffic reduction in the SDWSN field, two of which are that it is still a highly unexplored area of research and that while we aim to reduce control traffic as much as possible it is important to consider the network performance trade-off that may arise therein.

Acknowledgement

This work is based on the research supported in part by our industry partner Telkom. The grant holder acknowledges that opinions, findings and conclusions or recommendations expressed in any publication generated by this research are that of the author(s) and that our industry partner accepts no liability in this regard.

References

[1] B. Galloway and G. P. Hancke, "Introduction to industrial control networks," *IEEE Communications surveys & tutorials*, vol. 15, no. 2, pp. 860–880, 2013.

[2] G. Hancke, B. Silva, G. Hancke Jr *et al.*, "The role of advanced sensing in smart cities," *Sensors*, vol. 13, no. 1, pp. 393–425, 2013.

[3] M. Ndiaye, G. Hancke, and A. Abu-Mahfouz, "Software defined networking for improved wireless sensor network management: A survey," *Sensors*, vol. 17, no. 5, p. 1031, 2017.

[4] H. I. Kobo, A. M. Abu-Mahfouz, and G. P. Hancke, "A survey on software-defined wireless sensor networks: Challenges and design requirements," *IEEE access*, vol. 5, pp. 1872–1899, 2017.

[5] T. Luo, H.-P. Tan, and T. Q. Quek, "Sensor openflow: Enabling software-defined wireless sensor networks," *IEEE Communications letters*, vol. 16, no. 11, pp. 1896–1899, 2012.

[6] B. T. De Oliveira, L. B. Gabriel, and C. B. Margi, "Tinysdn: Enabling multiple controllers for software-defined wireless sensor networks," *IEEE Latin America Transactions*, vol. 13, no. 11, pp. 3690–3696, 2015.

[7] T. Luo, H.-P. Tan, P. C. Quan, Y. W. Law, and J. Jin, "Enhancing responsiveness and scalability for openflow networks via control-message quenching," in *2012 International conference on ICT convergence (ICTC)*. IEEE, 2012, pp. 348–353.

[8] S. Bera, S. Misra, S. K. Roy, and M. S. Obaidat, "Soft-wsn: Software-defined wsn management system for iot applications," *IEEE Systems Journal*, vol. PP, no. 99, pp. 1–8, 2016.

[9] F. F. J. Lasso, K. Clarke, and A. Nirmalathas, "A software-defined networking framework for iot based on 6lowpan," in *Wireless Telecommunications Symposium (WTS), 2018*. IEEE, 2018, pp. 1–7.

[10] A. R. Curtis, J. C. Mogul, J. Tourrilhes, P. Yalagandula, P. Sharma, and S. Banerjee, "Devoflow: Scaling flow management for high-performance networks," in *ACM SIGCOMM Computer Communication Review*, vol. 41, no. 4. ACM, 2011, pp. 254–265.

[11] M. Yu, J. Rexford, M. J. Freedman, and J. Wang, "Scalable flow-based networking with difane," *ACM SIGCOMM Computer Communication Review*, vol. 41, no. 4, pp. 351–362, 2011.

[12] M. Obadia, M. Bouet, J.-L. Rougier, and L. Iannone, "A greedy approach for minimizing sdn control overhead," in *Proceedings of the 2015 1st IEEE Conference on Network Softwarization (NetSoft)*. IEEE, 2015, pp. 1–5.

[13] H. I. Kobo, G. P. Hancke, and A. M. Abu-Mahfouz, "Towards a distributed control system for software defined wireless sensor networks," in *IECON 2017-43rd Annual Conference of the IEEE Industrial Electronics Society*. IEEE, 2017, pp. 6125–6130.

[14] L. Galluccio, S. Milardo, G. Morabito, and S. Palazzo, "Sdn-wise: Design, prototyping and experimentation of a stateful sdn solution for wireless sensor networks," in *Computer Communications (INFOCOM), 2015 IEEE Conference on*. IEEE, 2015, pp. 513–521.

[15] R. Friedman and D. Sainz, "An architecture for sdn based sensor networks," in *Proceedings of the 18th International Conference on Distributed Computing and Networking*. ACM, 2017, p. 20.

[16] A. Asaduzzaman, A. Almohaimeed, and K. K. Chidella, "Shared entry logger to eliminate duplicate requests to sdn controller," in *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*. IEEE, 2019, pp. 0579–0584.

[17] H. I. Kobo, A. M. Abu-Mahfouz, and G. P. Hancke, "Fragmentation-based distributed control system for software defined wireless sensor networks," *IEEE Transactions on Industrial Informatics*, 2018.

Musa Ndiaye, received his BEng in Electrical/Electronics Engineering from the Copperbelt University (Zambia) in 2011. He then obtained his MSc in Microelectronic and Communications Engineering from the University of Northumbria at Newcastle (United Kingdom) in 2013. He is currently a PhD student with the Advanced Sensor Networks group at the University of Pretoria (South Africa).

Gerhard P. Hancke, is a Professor at UP. He is recognized internationally as a leading Scholar in Industrial Wireless Sensor Networks (IWSN). He co-edited a textbook IWSN: Applications, Protocols, and Standards, (2013), the first on the topic. His IWSN paper in the IEEE Trans. Ind. Informat. attracted 1500 citations so far.

Adnan M. Abu-Mahfouz, is currently a Principal Researcher at the Council for Scientific and Industrial Research (CSIR), Research and Innovation Associate, Tshwane University of Technology, and also an extraordinary Faculty Member with the University of Pretoria. His research interests are wireless sensor and actuator network, low power wide area networks, software-defined wireless sensor network, cognitive radio, network security, network management, and sensor/actuator node development.