International Journal of Engineering & Technology, 7 (1.2) (2018) 229-234

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Software – defined networking based secure routing in mobile ad hoc network

B. V. V. S. Prasad [1]*, Sd. Salman Ali [2]

[1] *Department of Computer Science and engineering , DRK College of Engineering and Technology, Jntuh, Bowrampet, Hyderabad, India*

[2] *Department of Computer Science and Information Sciences, College of Science and Arts, Al Jouf University, Tabarjal, Kingdom of Saudi Arabia*

**Corresponding author E-mail: prasad_bvvs2004@yahoo.co.in*

Abstract

Traditional communication networks can be leveraged by separating controlling functions from forwarding functions using emerging technology known as Software Defined Networking (SDN). Though SDN has been around for some years, it was mostly limited to wired networks. Of late, it is being adapted to wireless networks. The programmable interface with decoupled controller can be used with MANET to integrate with other networks besides controlling it well. Both control and security are inevitable for the successful implementation of SDN in wireless networks. Towards this end, in this paper we implemented SDN based MANET for secure routing. Open Flow is used for implementing SDN controller while IDC is used for securing communications. Our framework is evaluated with NS3 simulations that reveal significant performance improvement when compared with traditional ad hoc networks that do not use SDN. This is achieved as SDN controller can quickly adapt to changed topologies due to node mobility.

Keywords: *Id-Based Cryptography; Software-Defined Networking; Secure Routing; Manet Colon.*

1. Introduction

Software Defined Networking (SDN) is an emerging architecture which decouples forwarding functions and network control thus it enables network control to be a programmable for network services and applications. It is cost-effective, adaptable, manageable, and dynamic in nature besides its suitability for today's high-bandwidth applications. The traditional architecture of networks is static and new computing trends like changing traffic patterns, consumerization of IT, rise of cloud services and big data demand a new paradigm to handle them. This is the rationale behind the need for SDN, which is the paradigm shift in controlling networks and underlying services and applications. The limitations of the traditional networks include vender dependence, inability to scale, and complexity [1]. Sukaridhoto [10] opined that SDN is one of the approaches used to improve performance in real time applications.

Mobile Ad Hoc Network (MANET) is a collection of nodes which is widely used for communications in case emergencies. It is used in both civilian and military applications [2], [13], [14]. The integration of SDN with MANET has very useful utility in communication networks. Towards this end, in [15] software defined networking was explored as an upcoming possibility that can help in having the flexible, reliable and programmable controller. Most of the decision making can be separated from the actual forwarding functions of network by the decoupling controller from the rest of the network. This is the motivation behind this research work, which is aimed at building a protocol based on SDN in MANET for military usage.

2. Literature review

This section provides the review of literature pertaining to SDN and its application to MANET. Mendonca et al. [1] focused on adapting SDN for heterogeneous networks. They considered two MANET networks connected through the Internet. One MANET is based on the traditional scenario while the other one is based on SDN scenario is described here. In the traditional scenario, Bob's device can act as the gateway. However, the service provider of mobile network is not aware about the existence of Alice. Internet Service Provider (ISP) can't apply quality of Service (QoS) rules and cannot control the bandwidth of devices in MANET [1]. Only Bob is made responsible for the traffic of Alice as Bob's acts as the gateway. In SDN scenario, there is a controller who can take care of runtime requirements of the MANET devices. For instance, it is aware of Alice as well. The separation of network controlling from forwarding hardware makes it flexible to take care of QoS requirements and improve performance as the controller is programmable. Heterogeneous environment is used, which comprises of traditional scenario and SDN scenario. As there is the Internet connecting two MANETs, it makes it a networking environment that appears in the real world and fully connected world. From this network, it can be understood how the SDN helps to separate network controlling activities to leverage the performance [1]. Similar kind of research was done by Mendonca et al. [9].

Santos, Nunes and Obraczka [3] proposed a novel approach for capacity sharing based on software defined networking. The research was done in hybrid networks. Their approach has underlying security mechanisms for having secure communications in

hybrid networks besides being able to have capacity sharing. Hu et al. [4] proposed an SDN based architecture for Vehicular Ad Hoc Network (VANET). They used OpenFlow [5], [6] standard for implementing SDN concept. Open Flow could provide the secure communication channel besides providing a programmable interface. Qin et al. [7] proposed SDN based framework for the Internet of Things (IoT). Their controller architecture has many services, tasks, devices and networks besides flow scheduling, solution specification, task-resource matching, and administration. Kaplan et al. [8] proposed a communication layer in Wireless Sensor Network (WSN) with software – defined networking concept. This led to efficient, evolvable network with high capabilities. Acceleration in networks can be achieved by using SDN [11], [12].

SDN is considered as an upcoming Internet architecture that can provide the plethora of advantages to communication networks [16]. Jacobsson et al. [17] adapted software defined networking concept to WSN. They proposed an architecture that is based on SDN for WSN. The SDN layers include application layer, control layer and infrastructure layer. The local controllers are coordinated by the SDN central controller for efficient communications. Salsano et al. [18] proposed a framework for Wireless Mesh Network (WMN) based on SDN with scenarios such as merging and partitioning. In their proposed network, controller, wireless mesh router (WMR), Gateway (GW) and client hosts are involved. There is a master selection process that for improving efficiency of the network. Li [19] proposed a framework based on SDN for efficient ambulance transportation. This framework could reduce time in transport and decision making. And the solution proves to be feasible for real world implementation.

Albanese et al. [20] explored moving target defense mechanism in MANET. They employed the concept of SDN for flexible and reliable outcomes as intended by such application in the real world. Their solution was robust against Sybil and other attacks. Foster et al. [21] provided a good overview of the languages that can be used to define the functionality for SDN, which controls networks. OpenFlow is one such API that could be used to do so. A good survey of SDN is found in [22] where insights on the concept are. Afaq et al. [23] found that SDN can be used to form a standard to flow detection, their marking and mitigation. Mitchiner et al. [24] provide a plethora of use cases that can be used to leverage networks based on SDN. Detti et al. [25] focused on SDN for WMN based on OpenFlow standards.

3. Proposed architecture

This section provides the scenario in which SDN is used. MANET is associated with a controller. The MANET itself can be interlinked with other networks in the real world. This scenario shows the fully connected world through the Internet. Thus the scenario shown in Figure 1 caters to both infrastructure less and infrastructure networks. The MANET devices denoted as Alice and Bob are considered to describe the proposed secure routing, and the need for SDN based scenario.

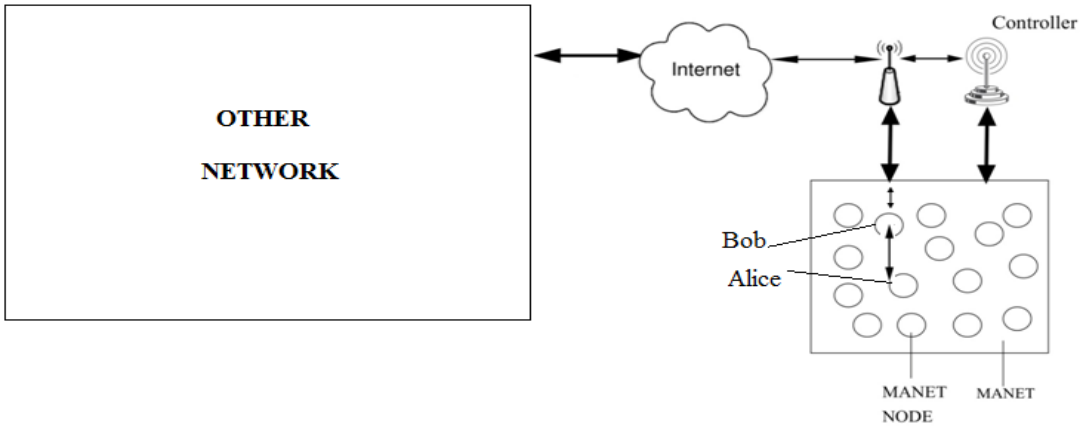

Fig. 1: SDN Enabled MANET.

The node denoted as Bob is considered a gateway node and other nodes such as Alice is considered user node. Here the forwarding activities and controlling activities are clearly separated where the controller is aware of the presence of user nodes as well. The controller is programmable and can be used to have many features, including sharing of resources. Opn Flow [26] is the standard protocol used to achieve this kind of architecture with a controller. Having provided the scenario the aim of the paper is to demonstrate the ID-based cryptography for secure communications in MANET with SDN controller. Then the results are compared with MANET without SDN controller. In our framework, we used the same notations as found in [3].

3.1. ID-based cryptography

To identify based cryptography (IBC) [27] originally proposed by Shamir can simplify the public key cryptography. It allows users to compute the public key from his/her publicly known identity such as email id. This will avoid expensive online certification verification. Moreover, a user requires only the publicly known identity of the recipient. Thus cryptographic primitives are made simple with IBC. The public key of any user is associated with an identity. Then it is essential to have the corresponding secret key. Here private key generator (PKG) comes from the picture. Figure 2 illustrates ID-based secure communication.

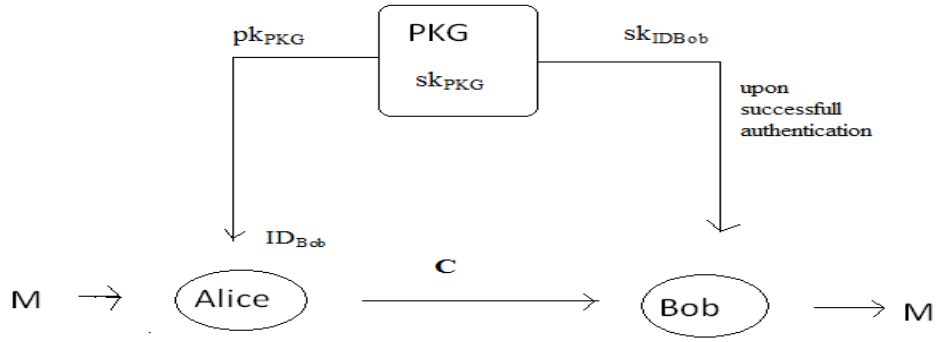

Fig. 2: Shows ID-Based Secure Communication.

All secret keys can be computed by the private key generator. The PKG contains its secret key named master secret key. Besides, it also has public key of the user to whom it needs to communicate. Here there are some advantages in having controller and PKG. We assume that controller is trusted which can provide programmable interface for management tasks. Thus it is possible to incorporate IBC into controller with respect to generation of keys.

3.2. Framework for secure communication with SDN

The end to end security is achieved in the proposed SDN based MANET using IDC. The entities involved in the secure communication are Alice, Bob, OpenFlow Access Point, and controller as shown in Figure 3. The message exchange among them is described here prior to describing the complete framework. Alice sends request to Bob. There is formal handshaking procedure between Alice and Bob. Bob sends packet-in message to controller to enable it to update its flow table to all parties concerned. Once authentication is done, Alice can agree shared keys with controller and AP using symmetric cryptography.

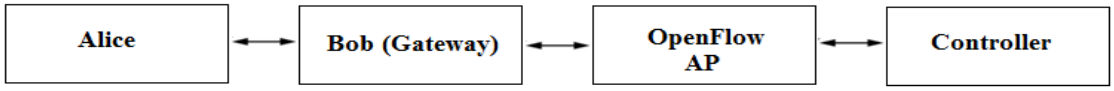

Fig. 3: Shows Entities among which End-to-End Security Is Provided.

In order to achieve secure communication different phases are required such as setup, handshaking, and authenticated key-agreement.

3.3. Setup

Since the PKG functionalities are equipped with controller, it plays a role in setup phase. Once public keys are computed from identities and map them in such a way that any node can obtain any other node's public key. The controller has master secret key and it can generate a private key for each node. Controller provides the private key for all the nodes in the MANET.

3.4. Handshaking

When Alice makes a request to Bob, Alice needs to respond to a challenge so that Bob can confirm the identity of Alice. It is important to keep in mind that both Alice and Bob should know each other's identity in order for authentication and exchanging messages. Thus then can generate a common shared key and both can perform encryption and decryption operations. A counter is used by Bob in order to protect the communication from replay attacks. The detailed procedure for handshaking is illustrated in Figure 4 which we have taken from [3].

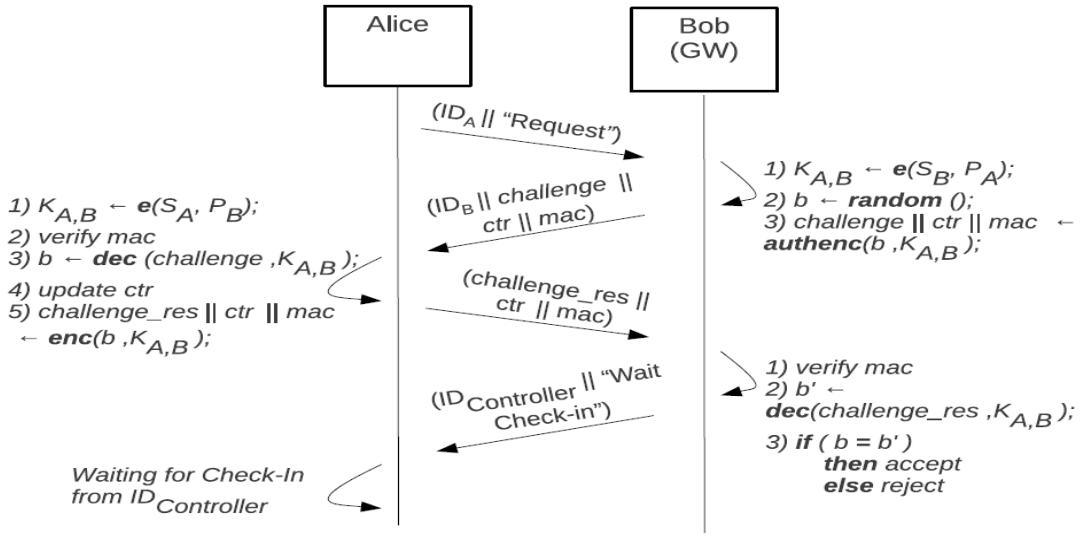

Fig. 4: Shows Handshaking Details.

As can be seen in Figure 4, there is authentication process between the two parties and the handshaking is part of it which also includes encryption and decryption procedures. There is a series of communication between the parties until the handshaking process

is completed. Once it is done, these two parties can participate in authenticated key agreement shown in Figure 5. We used the authenticated key-agreement procedure followed in [3]. Here Alice, after authentication, establishes pair wise keys with OpenFlow AP and controller.

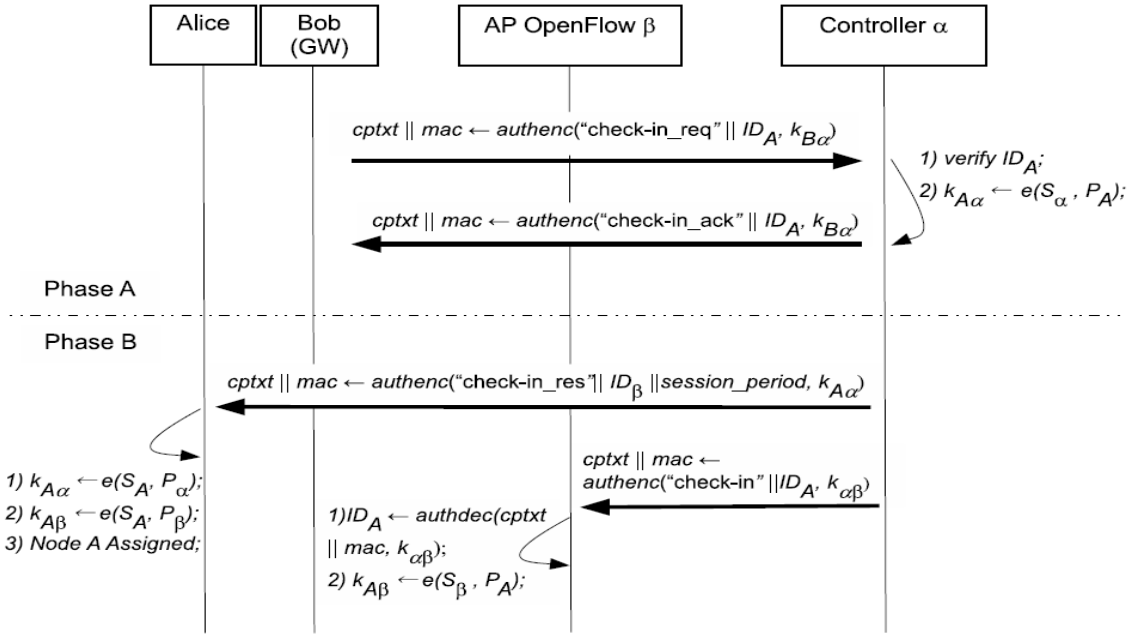

Fig. 5: Authenticated Key-Agreement.

After completion of handshaking, Alice establishes pair wise keys with OpenFlow AP and controller. This enables Alice to send secure messages to controller that cannot be decrypted by Bob. With a shared key with controller, Alice can prove her identity. This can also prevent malicious Bob (assumption) from pretending to be gateway for MANET devices that do not actually exist. As the SDN is based on OpenFlow controller and the controller is equipped with PKG capabilities, secure end to end communication is made possible.

4. Experimental results

Experiments are made with NS3 simulations in order to demonstrate the proposed framework. The ability to provide SDN based MANET that can show secure communications besides separating controlling functionalities is the important contribution in this paper. The results are analyzed in terms of secure communications, packet delivery ratio (PDR), and controller control traffic. Besides we compared our results with other MANET scenarios where SDN is not used. The scenarios for comparison are taken from [28]. The controller traffic is mostly generated by SDN controller only.

As shown in Figure 6, the PDR is presented in vertical axis while the horizontal axis shown the node mobility. There are two important observations revealed in the graph. First, the PDR is dropped when node speed increases. Second, the PDR is dropped when number of nodes is decreased. The reason behind this is that when no path is found between sender and receiver the routing fails. Both the factors contribute to the situation where a valid path is not found.

As shown in Figure 7, the control traffic is generated by SDN controller. The results reveal that more control traffic is required when number of nodes increases and node mobility is increased. Path finding issues can have impact on such traffic as expected.

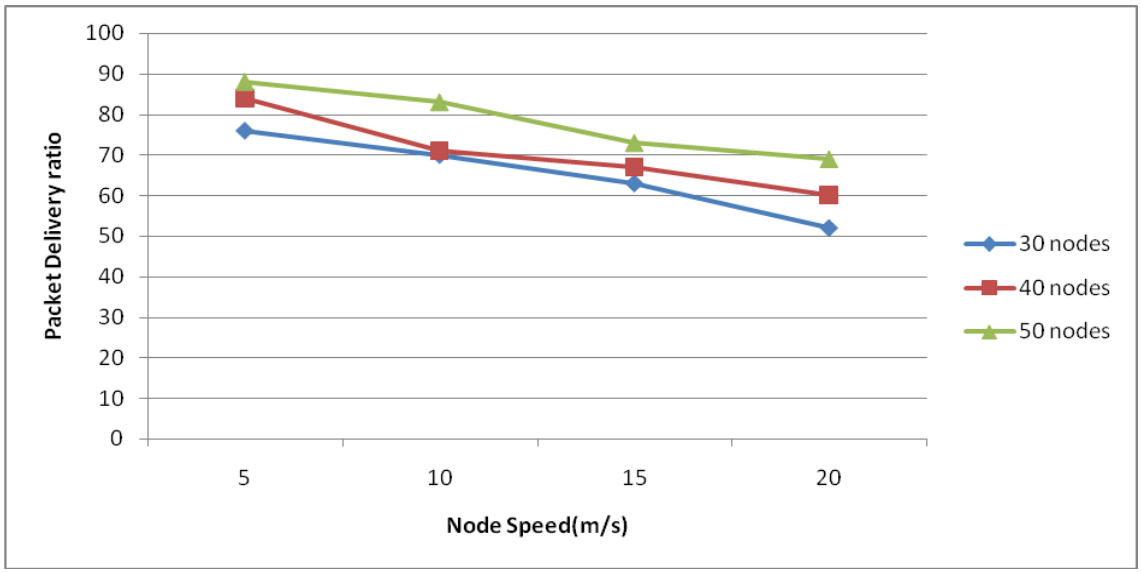

Fig. 6: PDR under Different Node Mobility.

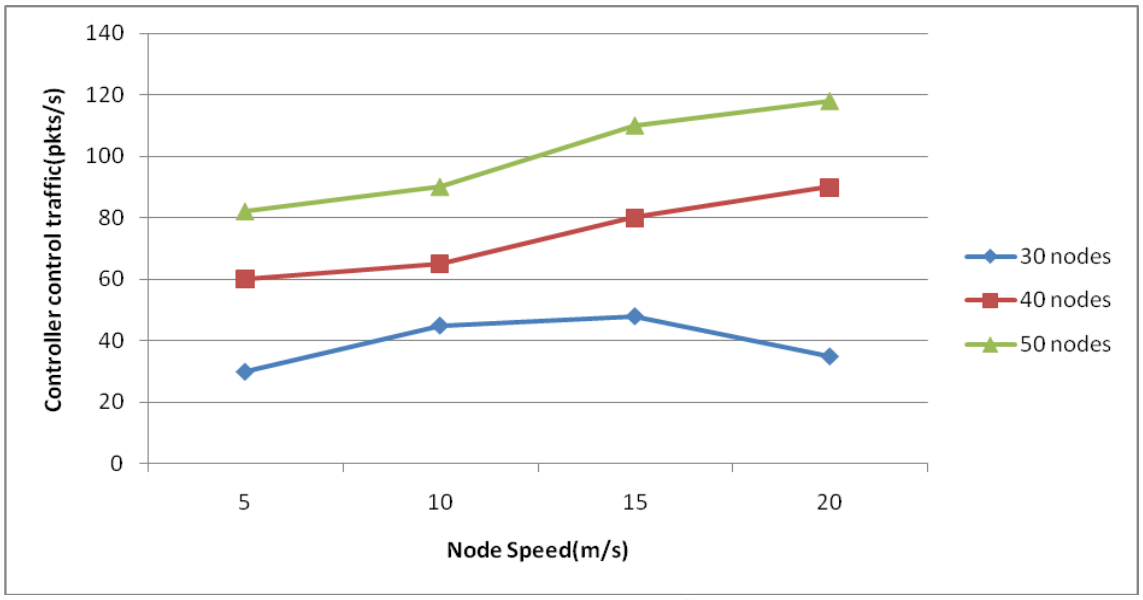

Fig. 7: Controller Control Traffic.

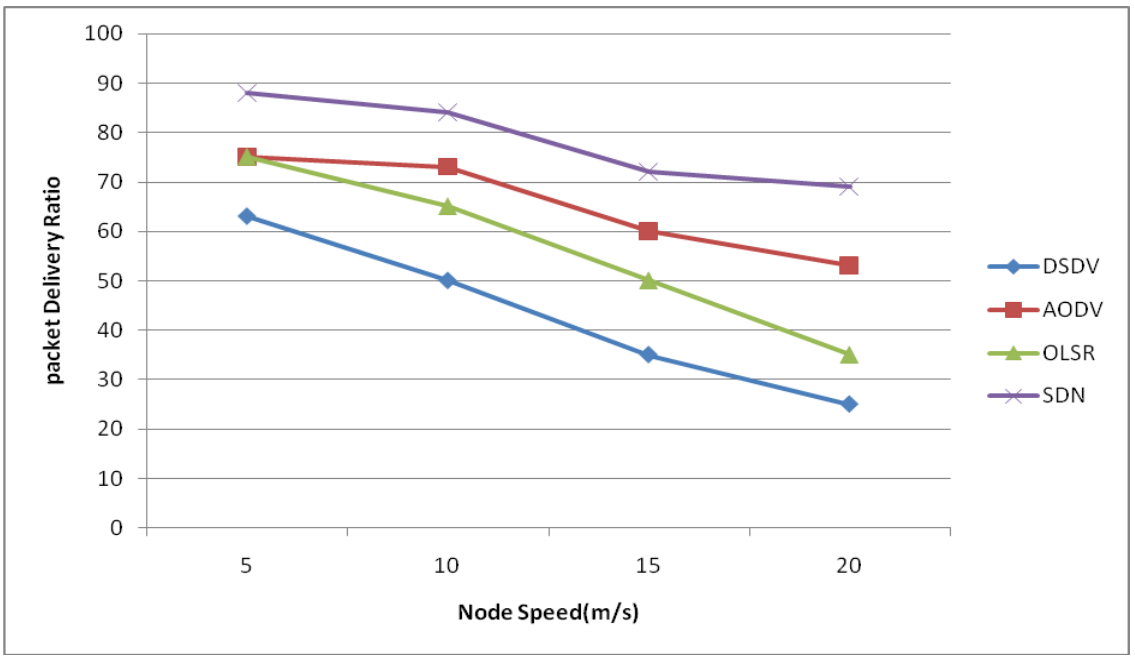

Fig. 8: PDR Comparison of SDN with Traditional Ad Hoc Routing.

As shown in Figure 8, it is evident that the SDN performance with respect to PDR is more when compared with traditional ad hoc routing protocols. The reason behind this is that SDN based MANET can respond quickly with topology changes. As the nodes are with mobility, the capacity to quickly adapt to new topology is the key contributor to the superior performance of SDN based MANET. Due to the fast response to the controller, the control messages are increased as shown in Figure 7. Since SDN knows user nodes and it can be programmed to have full control over the network, it paves way for high performance in MANET besides being able to realize the full vision of real-world connectivity with other networks through the Internet.

5. Conclusions and future work

In this paper we studied, the emerging technology named Software Defined Networking. The SDN can help to control networks like MANET from outside by decoupling controlling actions delegated to the controller. We are motivated by the fact that SDN is mostly limited to wired networks and adapting it to MANET can provide the flexible and efficient interface with the vision of fully the connected-world through the Internet. In order to realize this, we proposed a framework and implemented SDN controller using OpenFlow standard. The MANET scenario with SDN is demonstrated with NS3 simulations. The mobility feature of MANET and the controlling functions are studied. The results revealed that the MANET with SDN outperformed many other traditional ad hoc networks in terms of the packet delivery ratio. The rationale behind this is that, the SDN controller could adapt to topology changes quickly and ensure efficient routing in MANET. The results also revealed the reason behind reduced PDR due to path finding dynamics. In future, we intend to continue our research on SDN based MANET with different real-world applications. Another future direction is to incorporate an enhanced IDC scheme with the SDN controller and test its robustness against various attacks in MANET.

References

[1] Marc Mendonca, Bruno Nunes Astuto, Katia Obraczka, Thierry Turletti. (2013). Software Dened Networking for Heterogeneous Networks. HAL, p.12-17.

[2] Jun-Zhao Sun. (2001). Mobile Ad Hoc Networking: An Essential Technology for Pervasive Computing. IEEE, p.859–876. https://doi.org/10.1109/ICII.2001.983076.

[3] Mateus A. S. Santos. (2013). Software-Defined Networking Based Capacity Sharing in Hybrid Networks. IEEE, p.25-34. https://doi.org/10.1109/ICNP.2013.6733664.

[4] Ian Ku, You Lu, Mario Gerla. (2014). Towards Software-Defined VANET: Architecture and. IEEE, p.12-17. https://doi.org/10.1109/MedHocNet.2014.6849111.

[5] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, "Openflow: enabling innovation in campus networks," SIGCOMM Comput. Commun. Rev., vol. 38, no. 2, pp. 69–74, 2008. https://doi.org/10.1145/1355734.1355746.

[6] OpenFlow Switch Specification, Version 1.4.0 (Wire Protocol 0x05). [Online]. Available: https://www.opennetworking.org/images/stories/downloads/sdn-resources/onf-specifications/openflow/openflow-specv1.4.0.pdf.

[7] Zhijing Qin, Grit Denker§, Carlo Giannelli, Paolo Bellavista, Nalini Venkatasubramanian. (2014). A Software Defined Networking Architecture for the Internet-of-Things. IEEE, p.213-313. https://doi.org/10.1109/NOMS.2014.6838365.

[8] Murad Kaplan, Chenyu Zheng, Matthew Monaco, Eric Keller, and Douglas Sicker. (2014). WASP: A Software-Defined Communication Layer for Hybrid Wireless Networks. ACM, p.23-33. https://doi.org/10.1145/2658260.2658263.

[9] Marc Mendonca,Katia Obraczka,Thierry Turletti. (2012). the Case for Software–Defined Networking in Heterogeneous Networked Environments. ACM, p.56-60. https://doi.org/10.1145/2413247.2413283.

[10] Sritrusta Sukaridhoto. (2013). A Study of Performance Improvement Methods for Real-time Applications in Wireless Mesh Networks. A Solutions, p.12-17.

[11] Rahul Dasharath Gavas,R. H. Vijaylaxmi2. (2014). A Review on the Acceleration in Networking Fostered by Software Defined Networking.International Journal of Advance Research in Computer Science and Management Studies. 2 (3), p.213-313.

[12] Usama Mehboob, Junaid Qadir, Salman Ali, and Athanasios Vasilakos. (2014). Genetic Algorithms in Wireless Networking: Techniques, Applications, and Issues. A Solutions, p.56-60.

[13] Pieter Kleer. (2015). Distributed route discovery in communication networks using neighbour information. ACM, p.32-44.

[14] DAN L. BuRK. (1993). PATENTS IN CYBERSPACE: TERRITORIALITY AND INFRINGEMENT ON GLOBAL COMPUTER NETWORKS. A Solutions. 68 (1), p.23-33.

[15] Rahul Dasharath Gavas,R. H. Vijaylaxmi2. (2014). A Review on the Acceleration in Networking Fostered by Software Defined Networking.International Journal of Advance Research in Computer Science and Management Studies. 2 (3), p.213-313.

[16] Stefano Salsano, Giuseppe Siracusano, Andrea Detti, Claudio Pisa, Pier Luigi Ventre, Nicola Blefari-Melazzi. (2014). Controller selection in a Wireless Mesh SDN under network partitioning and merging scenarios.Software Defined Networking, p.25-34.

[17] Depeng Li. (2015). Poster: A Time-Saving Scheme for Ambulance Transportation with Support of Software-Defined Networking.Department of Information and Computer Sciences, p.213-313.

[18] Massimiliano Albanese, Alessandra De Benedictisy, Sushil Jajodia, and Kun Sun. (2013). A Moving Target Defense Mechanism for MANETs Based on Identity Virtualization. A Solutions, p.56-60. https://doi.org/10.1109/CNS.2013.6682717.

[19] Nate Foster, Michael. Freedmany, Arjun Guha, Rob Harrisonz, Naga Praveen Kattay, Christopher Monsantoy, Joshua Reichy, Mark Reitblatt, Jennifer Rexfordy, Cole Schlesingery, Alec Story, and David. (2013). Languages for Software-Defined Networks. ACM, p.12-17. https://doi.org/10.1109/MCOM.2013.6461197.

[20] Bruno Astuto A. Nunes, Marc Mendonca, Xuan-Nam Nguyen, Katia Obraczka, and Thierry Turletti. (2014). A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks.ACM, p.23-33.

[21] Muhammad Afaq, Shafqat Rehma, Wang-Cheol Song. (2015). Large Flows Detection, Marking, and Mitigation based on sFlow Standard in SDN. Journal of Korea Multimedia Society. 181 (2), p.12-17. https://doi.org/10.9717/kmms.2015.18.2.189.

[22] Mark "Mitch" Mitchiner,Reema Prasad. (2014). Software-Defined Networking and Network Programmability: Use Cases for Defense and Intelligence Communities. Cisco, p.56-60.

[23] Ahyoung Lee1 • Ilkyeun Ra2. (2015). Network resource efficient routing in mobile ad hoc wireless networks. Springer-Verlag Berlin Heidelberg, p.23-33.

[24] Haidong Wang, Brian Crilly, and Wei Zhao. (2007). Implementing Mobile Ad Hoc Networking (Manet) Over Legacy Tactical Radio Links. Ieee, P.56-60. https://doi.org/10.1109/MILCOM.2007.4455103.

[25] Hanno Wirtz, Tobias Heer, Robert Backhaus, Klaus Wehrle. (2011). Establishing Mobile Ad-Hoc Networks in 802.11 Infrastructure Mode.ACM, p.213-313.

[26] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner, "Openflow: enabling innovation in campus networks," SIGCOMM Comput. Commun. Rev., vol. 38, no. 2, pp. 69–74, Mar. 2008. [Online]. Available: http://doi.acm.org/10.1145/1355734.1355746

[27] A. Shamir, "Identity-based cryptosystems and signature schemes," in CRYPTO, ser. LNCS, G. Blakley and D. Chaum, Eds. Springer Berlin Heidelberg, 1985, vol. 196, pp. 47–53.

[28] J. Broch, D. Maltz, D. Johnson, Y.-c. Hu, and J. Jetcheva. A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols. In Proceedings of the Fourth Annual ACMIIEEE International Conference on Mobile Computing and Networking (MobiCom'98), pages 85-97, Dallas, TX, October 1998. ACM. https://doi.org/10.1145/288235.288256.