JOURNAL OF INFORMATION SCIENCE AND ENGINEERING 37, 1335-1340 (2021)
DOI: 10.6688/JISE.202111_37(6).0008

Design and Performance Analysis of Wireless IPv6 for Data Exchange

OSAMAH IBRAHIM KHALAF[1,+] AND GHAIDA MUTTASHAR ABDULSAHIB[2]
[1]*Al-Nahrain Nanorenewable Energy Research Center*
Al-Nahrain University
Baghdad, 10072 Iraq
E-mail: usama.ibrahem@coienahrain.edu.iq; usama81818@gmail.com
[2]*Department of Computer Engineering*
University of Technology, Iraq
Baghdad, 10066 Iraq
E-mail: gh961@yahoo.com; 30834@uotechnology.edu.iq

The mobility of wireless nodes is one of the key issues of network communication significance and always has been. Researchers are empowered by the rapidly increasing in need of node mobility inside the network without having to lose any link or the data transfer. This report concentrated on the technological factors of WPIP*v*6. The primary objective of the Wireless Proxy Internet Protocol 6 (WPIP*v*6) is to minimize the problem of core system and enhance the node mobility on wireless devices. It is a based communication mobility protocol. We initiate by implementing negotiation concepts for key exchange protocols, attempting to change the defined systems to takes into consideration the safety of the cypher suite and negotiating versions in the TLS protocol.

Keywords: IP*v*6, authentication, wireless node, key exchange, protocol

1. INTRODUCTION

In developing or implementing such protocols, including the Domain Name System (DNS) [1] and the Transport Layer (TLS) [2], the transformation, insecure network protocols have indeed been driven mainly by discovering and effectively exploiting faults providing good analysis to show such a damaged reactive evolutionary process. The increasing numbers of networking and digital device assumes that the shift from IP*v*4 to IP*v*6 is inevitable for persons or groups. The deployment of IP*v*6 in most advanced smart devices has correspondingly been enhanced [3]. Initially, IP*v*4 and its laws restricting were to comprehend the World Wide Web [4]. The other one knows IP*v*6 and what benefits it tends to bring to the technological world. The next case would have been to discover out why the transition from IP*v*6 takes a long time. In the design and implementation of certain protocols, we identify several vulnerabilities that can be targeted by an attacker to perform various, which in many cases, major threats that undermine his important strategic objectives. The impact and applicability of our work enhance beyond the academic and extend, which included researchers, designers, and software implementers in the broader community of network protocols [5, 6].

Received September 17, 2020; revised October 10, 2020; accepted October 15, 2020.
Communicated by Amine Mohammed El Abdelli.
+ Corresponding author.

2. THEORETICAL RSSI MODEL

The implementation of IP*v*6 also addressed the problems, and the researchers represent various solutions to existing problems. Many investigators accepted the fact during the analysis could be discovered [7-9]. In order to provide significant-efficiency than the Ad hoc On-Demand Vector (AODV) algorithm [10-12], the author proposed a Micro Sensor Routing Protocol on the wireless connection. In the IP*v*4-UDP tunneling protocol; the researchers have proposed IP*v*6 to implement IP*v*6 in IP*v*3 and improved the packet's low latency in relay time from 9.76μs to 8.21μs for Miredo-relayed [13]. This Escort protocol has indeed been studied based on packet throughput with a capacity to cross symmetrical NATs of around 6U~10U and measures, sported motility, and multi-homing. The authors recommend an autonomous IPv6 address configuration for LoWPAN together with the AH & ESP and 6LoWPAN policy-based [14, 15].

3. IMPLEMENTATION OF WPIPv6

3.1 Network Installation

The WPIPv6 test-bed is created on the basis of WPIPv6's open-air implementation group. The system consists of the following entities, as mentioned in Fig. 1 Client Mobile Node (CMN), Wireless Access Point (WAP1, WAP2), Root Node (RN), and Wireless Node (WN) [16, 17].

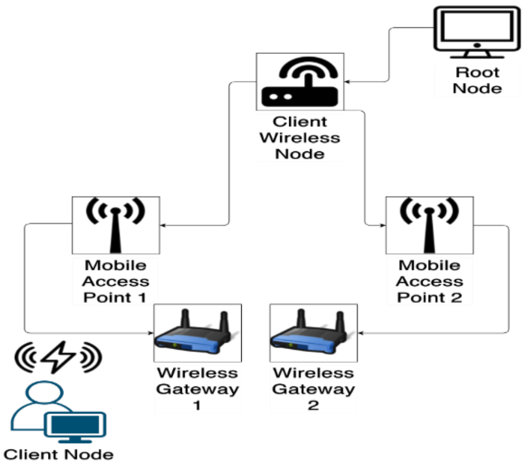

Fig. 1. Setup of WPIP*v*6 test bed.

4. PERFORMANCE EVALUATION

The main objective of the experiments carried out across the whole proposal is to examine and assess the actions of WPIP*v*6 in real-world scenarios. The objective of this experiment is to give you accurate knowledge of the restrictions of the WPIP*v*6 protocol, such as the delivery time, the packet delivery ratio, and the bandwidth transfer. The evaluation tests were performed in the following steps. A first step is an assessment without any improvements to the WPIP*v*6 protocol. The second step is to assess the proposed enhancements in order to check whether these variations overcome the WPIP*v*6 protocol weaknesses [18, 19].

4.1 Evaluation Environment

The proof of concept setup of WPIPv6 is performed with the help of an open-air group for WPIP*v*6. As can be seen in Fig. 4 CNM, WAP1, WAP2, RN, and WN, the testing setup comprises of the following entities [20].

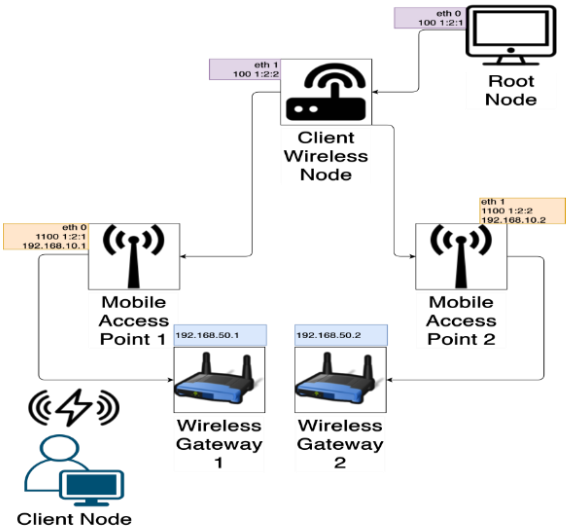

Fig. 4. WPI*v*6 network experimental configuration.

As proposed, version 10.04 of the UBUNTU System with kernel 2.26.35 is often used for networked devices, and Table 1 shows the details of the test-beds.

Table 1. Setting up the test-bed nodes for detailed machine.

Test Node	CPU	Primary Memory	OS	Software	Access Point
Client Node	Core i 3	4 GB	Linux	Free Radius Client	Wireless Port
Server Node	Core i 7	16 GB	Linux	Free Radius Server	Wireless Port

4.2 Time Synchronized Authentication Protocol (TSAP)

In order to have access to the performances and outcomes, we display the TSAP for authentication method network time synchronization. In the enhanced version fields of the NTP messages, TSAP messages are transported. TSAP allows a server to verify to a client using public-key certificates and exchanges of public key and guarantees that the packets haven’t altered in transit, using symmetrical encryption. We presume that an original off-band method for verification is visible as certificate recognition requires accurate clocks like most of the other authenticated clock synchronization protocols using public keys. That being said, future certificate checks can be conducted commonly after the initial synchronization with TSAP. In order to identify which TSAP cryptographic, data processing, and storage properties should attain, we implement IETF’s Information Document, Time Protocol Requirement for Packet-Switched Networks.

4.4 Time Delay Transfer and Packet Loss Tested in WPIP*v*6

The process is performed by sending or receiving a data packet between some of the WN and RN using the *Ping6* command. This study is required to determine the delay and packet loss during the transfer period. The WN links first to WAP1 under this case and then starts to send to the Root Node a particular data packet. The WN then disconnects from the WAP1 access link while trying to send the packets to RN and attaches to the WAP2 access link.

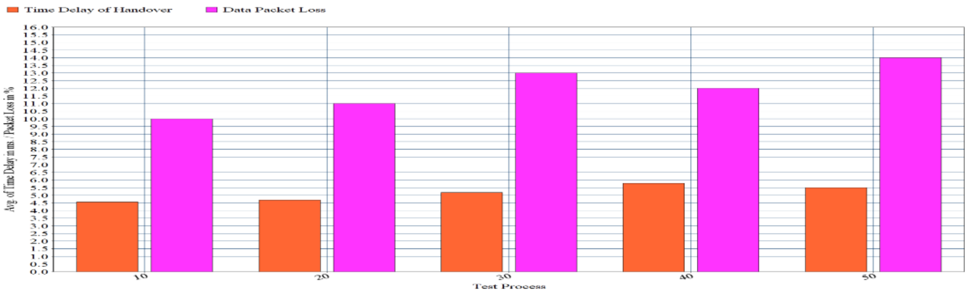

Fig. 5. Performance evaluation of time and packet loss ratio.

The aim of these measurements is not really to determine the relative time for the period of the transfer process, but also to estimate the PDR throughout that time, which can be seen in Fig. 5. In order to evaluate the loss of PDR, the Packet loss test was set up using *Ping6* commands.

5. CONCLUSION

IP is being used for the transmission of non-secure channels; an IP is important to ensure inter-Site communication. IP presents confidentiality, integrity, and authentication. This author proposes methods for modifying the boundaries of the WMIP*v*6. The work starts with WMIP*v*6 enforced in a testing room in order to compute the protocol’s measures in a real scenario. The installation is based on the test open-source performance regarding the WMIP*v*6 configuration when we introduced the new authenticated time synchronization protocol called TSAP, which is designed with a public-key infrastructure to securely synchronized a client’s and server’s times. During the first step, the time limit is done by decreasing the authentication procedures inside the movement of the network nodes on the domain.

REFERENCES

1. O. I. Khalaf, G. M. Abdulsahib, and B. M. Sabbar, "Optimization of wireless sensor network coverage using the bee algorithm," *Journal of Information Science and Engineering*, Vol. 36, 2020, pp. 377-386.
2. S. K. Prasad, J. Rachna, O. I. Khalaf, and D.-N. Le, "Map matching algorithm: Real time location tracking for smart security application," *Telecommunications and Radio Engineering*, Vol. 79, 2020, pp. 1189-1203.
3. O. I. Khalaf, G. M. Abdulsahib, H. D. Kasmaei, and K. A. Ogudo, "A new algorithm on application of blockchain technology in live stream video transmissions and telecommunications," *International Journal of e-Collaboration*, Vol. 16, 2020, pp. 16-32.
4. A. D. Salman, O. I. Khalaf, and G. M. Abdulsahib, "An adaptive intelligent alarm system for wireless sensor network," *Indonesian Journal of Electrical Engineering and Computer Science*, Vol. 15, 2019, pp. 142-147
5. K. A. Ogudo, M. J. Nestor, O. I. Khalaf, and H. D. Kasmaei, "A device performance and data analytics concept for smartphones' IoT services and machine-type communication in cellular networks," *Symmetry*, Vol. 11, 2019, p. 593.
6. O. I. Khalaf and G. M. Abdulsahib, "Frequency estimation by the method of minimum mean squared error and P-value distributed in the wireless sensor network," *Journal of Information Science and Engineering*, Vol. 35, 2019, pp. 1099-1112.
7. O. I. Khalaf and B. M. Sabbar, "An overview on wireless sensor networks and finding optimal location of nodes," *Periodicals of Engineering and Natural Sciences*, Vol. 7, 2019, pp. 1096-1101.
8. G. M. Abdulsahib and O. I. Khalaf, "An improved algorithm to fire detection in forest by using wireless sensor networks," *International Journal of Civil Engineering and Technology*, Vol. 9, 2018, pp. 369-377.
9. G. M. Abdulsahib and O. I. Khalaf, "Comparison and evaluation of cloud processing models in cloud-based networks," *International Journal of Simulation –Systems, Science & Technology*, Vol. 19, 2018, pp. 26.1-26.6.
10. O. I. Khalaf, G. M. Abdulsahib, and M. Sadik, "A modified algorithm for improving lifetime WSN," *Journal of Engineering and Applied Sciences*, Vol. 13, 2018, pp. 9277-9282.
11. N. Sulaiman, G. Abdulsahib, O. I. Khalaf, and M. N. Mohammed, "Effect of using different propagations of OLSR and DSDV routing protocols," in *Proceedings of IEEE International Conference on Intelligent Systems Structuring and Simulation*, 2014, pp. 540-545.
12. M. Küçük and F. Findik, "Selected ecological settlements," *Heritage and Sustainable Development*, Vol. 2, 2020, pp. 1-16.
13. M. Küçük and T. T. Karadayi, "An ecological settlement design for refugees in Kocaeli," *Heritage and Sustainable Development*, Vol. 2, 2020, pp. 69-88.
14. A. Çakır and E. F. Kurmuş, "Energy storage technologies for building applications," *Heritage and Sustainable Development*, Vol. 1, 2019, pp. 41-47.
15. O. F. Ulusoy and E. Pektaş, "Recent trends and issues in energy conservation technologies," *Heritage and Sustainable Development*, Vol. 1, 2019, pp. 33-40.
16. A. Husejinović, "Efficiency of commercial banks operating in federation of Bosnia and Herzegovina using DEA method," *Sustainable Engineering and Innovation*, Vol.

1, 2019, pp. 106-111.
17. H. K. Silman and A. E. Ali, "Breast cancer identification based on artificial intelligent system," *Sustainable Engineering and Innovation*, Vol. 2, 2020, pp. 109-118.
18. I. Al-Barazanchi and H. R. Abdulshaheed, "Designing a library management system for Gazi Husrev-beg library using data structure and algorithm," *Heritage and Sustainable Development*, Vol. 1, 2019, pp. 64-71.
19. H. R. Abdulshaheed, I. Al-Barazanchi, and M. S. B. Sidek, "Survey: Benefits of integrating both wireless sensors networks and cloud computing infrastructure," *Sustainable Engineering and Innovation*, Vol. 1, 2019, pp. 67-83.
20. M. A. M. Halilovic, "Potential of air quality improvements in Sarajevo using innovative architecture approach," *Periodicals of Engineering and Natural Sciences*, Vol. 5, 2017, pp. 128-135.

Osamah Ibrahim Khalaf is a Dr. in Al-Nahrain University at AlNahrain Nanorenewable Energy Research Centre. He has held many years of university-level teaching experience in computer science and network technology and has a strong CV about research activities in computer network.

Ghaida Muttashar Abdulsahib is a Dr. in Department of Computer Engineering/University of Technology, Iraq. She has held many years of university-level teaching experience in computer science and network technology and has a strong CV about research activities in computer network.