International Journal on Emerging Technologies **10**(2): 299-306(2019)

ISSN No. (Print) : 0975-8364
ISSN No. (Online) : 2249-3255

A Novel Block Chain-Based Approach for Secure Handoff in WMN with Reduced Authentication Delay

Suraj Malik[1] and Rakesh Kumar[2]
[1]Ph.D Scholar, Dr. A.P.J Kalam Technical University, Lucknow, (U.P.), India
[2]Professor, Madan Mohan Malviya University of Technology, Gorakhpur, (U.P.), India

(Corresponding author: Suraj Malik)
(Received 20 April 2019, Revised 18 July 2019 Accepted 26 July 2019)
(Published by Research Trend, Website: www.researchtrend.net)

ABSTRACT: Currently, Wireless mesh networks (WMNs) and Block Chain are two most prominent technologies in the telecommunication industry. WMN subsist of wireless mesh router (WMNR) and wireless mesh client (WMNC). WMN is a set of self-configured and self-organized nodes which ensure a free mobility, and a self-configuration of the diverse network apparatus, an enhanced quality of services, as well as an extensible area. Although, WMN extensively enhance the performance of wireless personnel area network (WPANs), wireless ad-hoc network (WANETs), wireless metropolitan area network (WMANs) and wireless local area networks) still mesh technology endures from various hitches such as security particularly in handoff phases and authentication delay during handoff procedure. This paper proposed a novel block chain-based approach to secure handoff process. Moreover, the proposed method reduced authentication delay during handoff procedure in wireless mesh network.

Keywords: Secure Handoff, Reduced Authentication Delay, Wireless mesh networks (WMNs), mesh router,

I. INTRODUCTION

Wireless mesh networks (WMNs) consists of two nodes namely as mesh router (MRs) and mesh client, where mesh router have nominal mobility and form the backbone of WMN though MCs are cellular phone, and entrée the network services via mesh routers as shown in fig. 1 [1]. In WMN the clients may exactly communicate with each other and forward the data packets to their destination nodes. Further, MR has no moderation on energy consumption and communication resources in comparison of MCs. Fig. 1 shows the existing wireless mesh network structure.

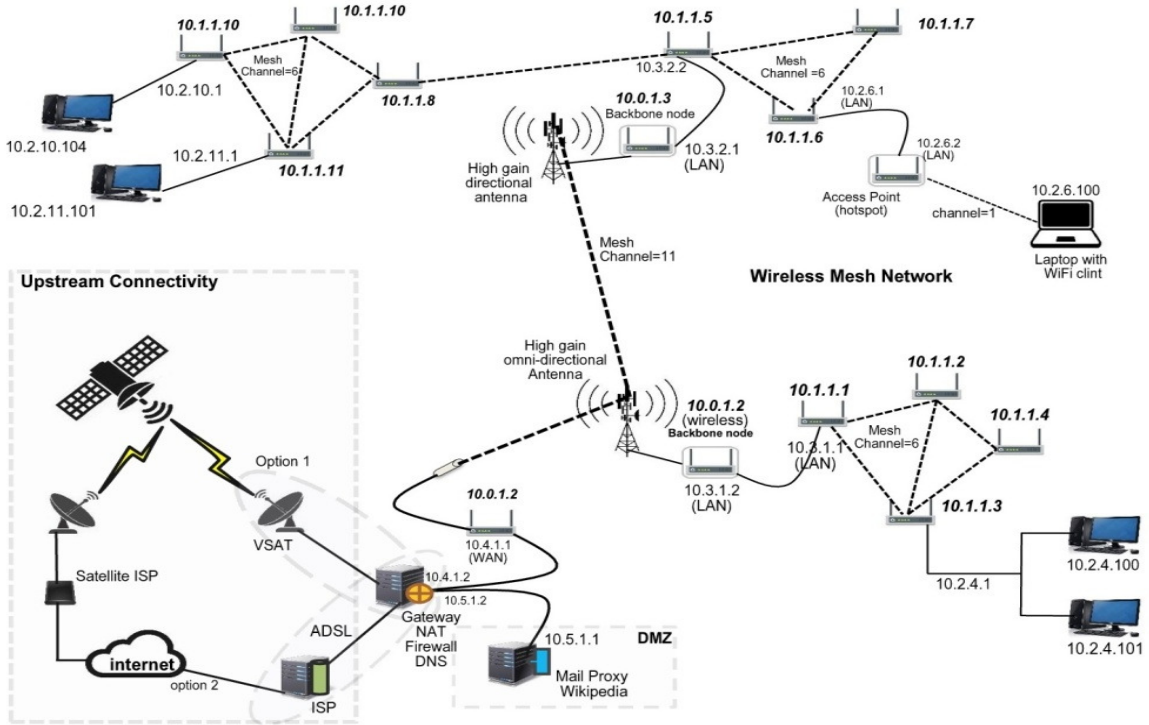

Fig. 1. Existing wireless mesh network architecture.

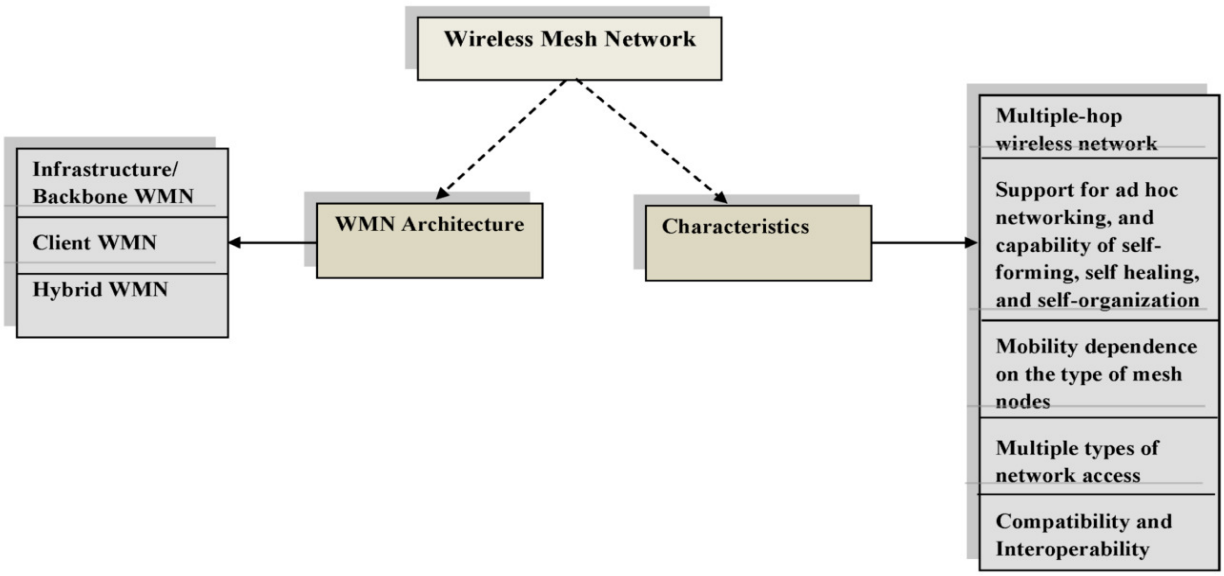

Fig. 2. Classification of wireless mesh network architecture.

Fig. 2 shows the three different types of network architecture for wireless mesh network named as Infrastructure/Backbone, Client WMN, and Hybrid WMN. Fig. 2 shows the various distinct characteristics of WMNs [1, 2] as well as it evaluated with conventional wireless networks. a) *Multi-hop WMN* is developed due to some hitch in the existing WMN thus; WMN is developed with extensive coverage range without coverage range without forfeit of channel competence. Non-line-of-sight (NLOS) connectivity provided by among the other users without direct-link-of sight (LOC). Therefore, to fulfill these objectives the mesh-styling multi-hopping is essential [3] with high throughput excepting libation efficient radio range by shorter link distances, less interfering between the nodes, and more proficient frequency re-use.

b*) Capability of self-forming, healing, organization as well as ad hoc networking support;*

The network efficiency enhanced by WMN through agile network structure, leisurely deployment, configuration, fault tolerance, and mesh connectivity.

Mobility dependence on the type of meshes nodes; Mesh routers generally have nominal mobility, while mesh clients can be immobile. C) WMN [4] support peer-to-peer communications, backhaul access to the internet and multiple kinds of network. Further, the amalgamation of WMN with other wireless networks accomplished other features such as it provides other network services to end-users.

The rest of the paper is organized as follow: Section 1 discusses the brief introduction on WMN Section 2 gives the briefs about architecture. Section 3 detailed the handoff procedure. Section 4 describes the related work about WMN. Section 5 related to the problem formulation while Section discussed proposed approach. Finally, Section 7 concludes the entire manuscript.

The technical contributions of this manuscript are fourfold which are described as follows:

- To fast handoff by block chain
- Reduced authentication delay with the help of block chain
- Proposed approach gives an optimal solution regarding malicious threat during handoff process as well as to reduce authentication delay.
- Proposed approach secure data during handoff process.

II. ARCHITECTURE OF A WMN

Fig. 3, 4, and 5 depicts the types of wireless mesh network architecture which is classified as infrastructure/Backbone WMN, Client WMNs, and Hybrid WMN. Infrastructure WMN; it comprises mesh routers structuring an infrastructure for clients that connect to them. Although, distinct types of radio technologies used for creating WMN but most of the technology used technology named as IEEE 802.11. A mesh of self-configuring and self-healing links designed by and the mesh routers. Further, the mesh routers connected to the internet by gateway functionality. Infrastructure WMN shown in Fig. 3.

(b) Client WMN; among devices are connected by peer-to-peer networks in client meshing.

The actual network comprises by client nodes which performs routing and configuration functionalities in the client WMN architecture. Moreover, the end user applications also provided to customers by this architecture. Thus, in Client WMN network mesh router is not necessitated. Fig. 4 demonstrates the basic structure of WMN.

(c) Hybrid WMN; it is the amalgamation of infrastructure and client meshing as shown in figure 5. Mesh clients can access the network through mesh routers as well as directly meshing with other mesh clients. While the infrastructure provides connectivity to other networks such as the Internet, Wi-Fi, WiMAX, cellular, and sensor networks; the routing capabilities of clients provide improved connectivity, and coverage inside the WMN [1, 2].

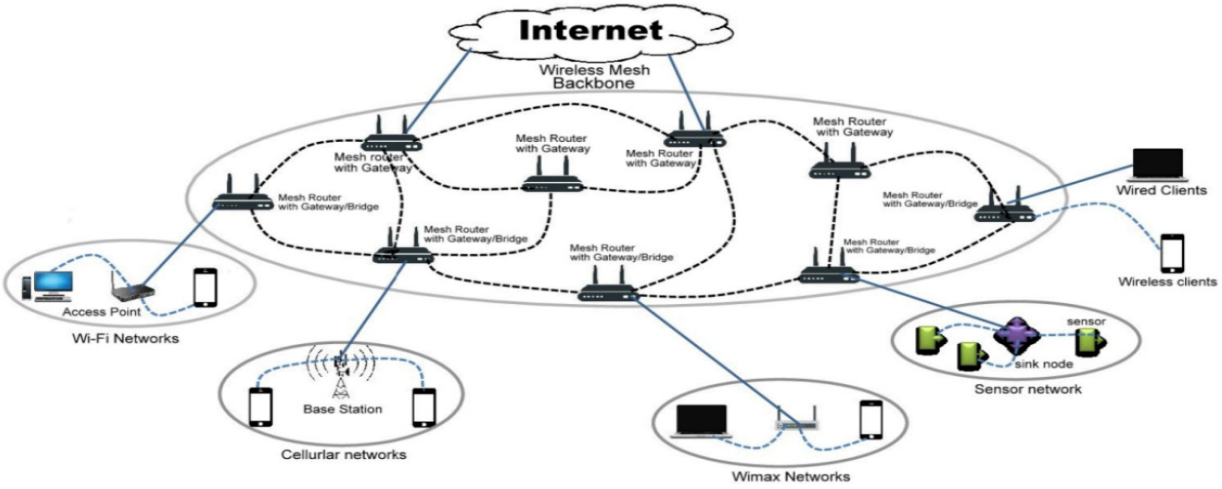

Fig. 3. Infrastructure wireless mesh network.

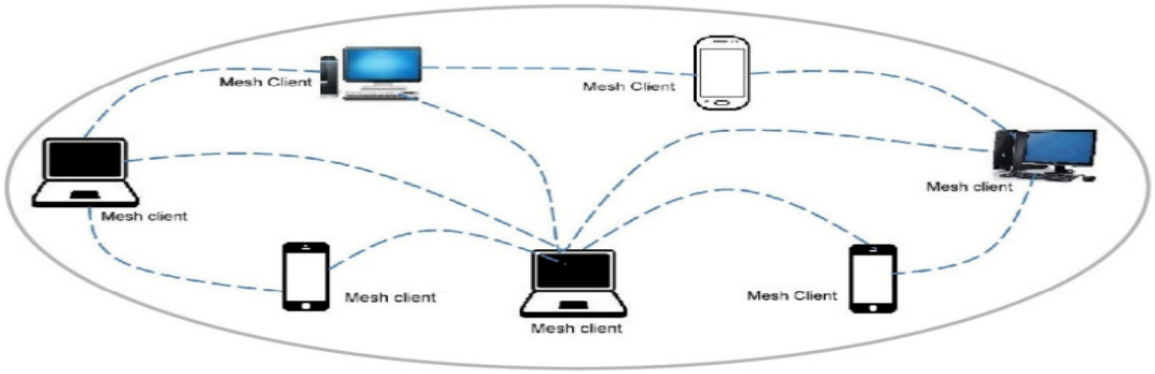

Fig. 4. Client wireless mesh network.

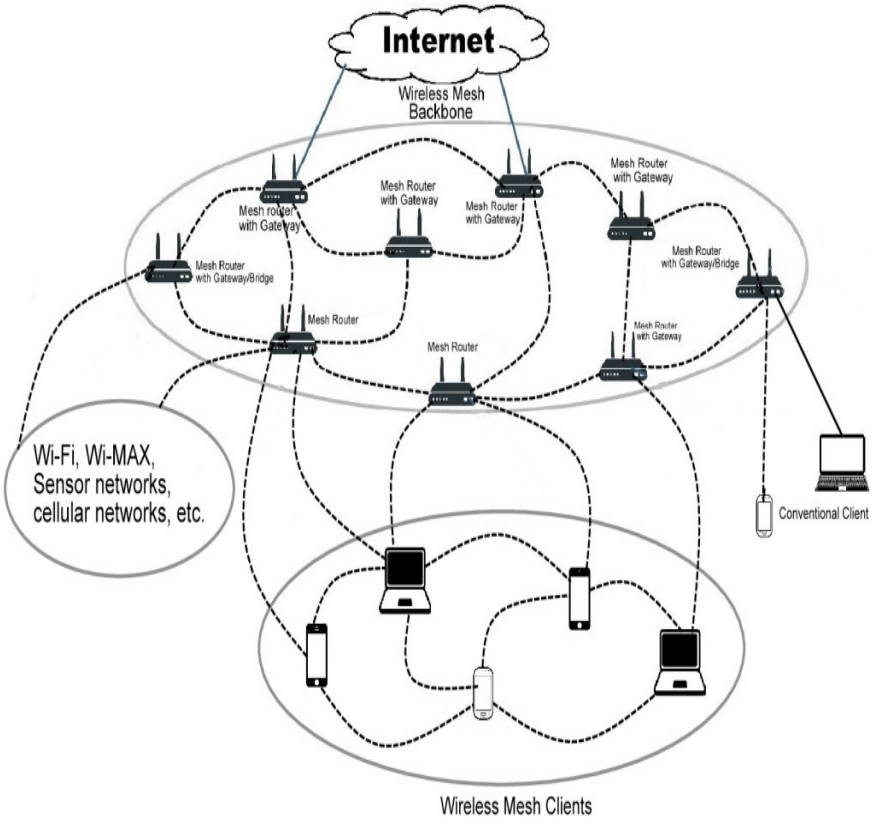

Fig. 5. Hybrid wireless mesh network.

In this paper a block chain-based methods has been proposed for securing handoff process, and reduce the authentication delay during handoff procedures.

III. HANDOFF IN WMN

Mesh clients necessitate changing their current access MR to a new on due to the mobility nature of users. Authors [5] defined handoff as connecting the new mesh router by send-off the present hand out router's range due to fall in signal attenuation during mobility. Let us consider this situation as when a MC moves into remote boundary of its serving HMR (home mesh router) the SNR (signal-to-ratio) incline because of signal attenuation. Hence, thus, the due to considerable falls in SNR ratio initiates the MC to explore a new foreign mesh router(FMR) having high-quality signal for enhanced services by eliciting the handoff process in the network. Due to dynamic, unstable, and limited nature of nodes create some security as well as performance concerns. Further, a substantial obstruction in handoff process may cause profuse concert apprehensions such as assaults and impediment. It is essential that roaming client should have sufficient avenue authentication with a short delay during handoff process with the strengthening for the roaming clients and for handoff networks.

Although, various handoff protocols have been anticipated in the existing research to diminish handoff latency. Figure 6 shows the handoff process. Xu et al. [6] have divided handoff process in two phases named as probe and re-authentication. In probe-phase the entire channel impeded successively by an MC to discover an MR with the high signal for the coupling. Therefore, the apprehension of "probe latency" relies on the number of the accessible channels. However, several researchers (have proposed various handoff latency in the literature [7, 8, 9]. The other phase is re-authentication which is similar as that of authentication. Moreover, this phase is affected by several factors named as congestion factor, range from AS, and an amount of authentication message sharing etc. In such case, the trust relationship is established by MC with the new MR and MC also performs key substances sources. While on the other side, MRs needs to couple with roaming client to share frames, the quality of service (QoS), communication context, etc. Therefore, re-authentication will induce a extensive delay which could not be ample for the present appliance. However, there are a number of consequence in handoff that accrues significant consideration [1] such as a) Multi-hop wireless authentication; the latency will further augment because of authentication flow in three-party handoff protocol require to go by multiple wireless hops on both wired and wireless links. It would be enviable if message are transmitted simply between two individual throughout handoff. b) Energy restraints; MC, are often power limited to support mobility while MR are capable for complex calculations and communications. Mesh routers should transmit maximum resource overwhelming procedures to a simple the lumber of mesh clients. c) Cooperation feature; in this feature MR transmit packets for the clients in a mutual way. Further, using the new router as a relay after handoff the roaming client can connect with the prior router. Consequently, a comprehensive authentication within the new router and the client is not essential. In this paper, we focused on a block-chain based approach for securing handoff process as well as to reduce authentication latency. Further, proposed approach also secure data.

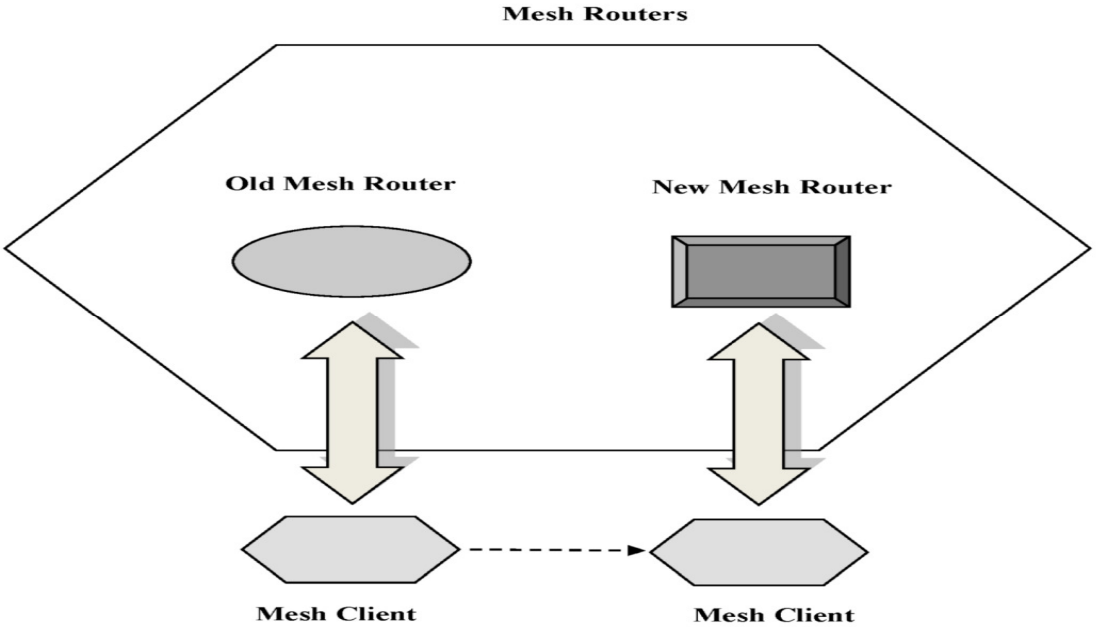

Fig. 6. Handoff process in WMNs.

IV. RELATED WORK

There are a number of approaches have been proposed in literature by various researchers for reduce handoff latency in WMN. Xu et al. [6] used ticket-based handoff authentication for WMN. In this method handoff latency reduced without involvement of third part as authentication server (AS). MC s directly authenticated by MRs by the tickets spawned by routers. Authors had used symmetric key encryption and focused on the reduction of re-authentication latency. Numerous

handovers and authentications in 5g small cells and HetNets thrash out by [10]. Moreover, they introduced software defined network (SDN) into 5G. The malicious free ambiance for mobile ad-hoc network offered by a trust scheme proposed by [11] Moreover, the authenticity of nodes impedes by anticipated structure via challenge response technique and then facilitates the trusted communication platform by giving PKI certificate to only authenticate nodes.

Two multi-hop authentication protocols proposed by Forsberg *et al.* [12] and Tseng *et al.* [13]. Further, in proposed method the client passing message via multiple hops to AS to authenticate itself. There are three handoff techniques exist in the literature [6] named as multi-hop, ticket-based and proactive. In multi hop approach roaming clients requires to re-authenticate itself to AS. Although, the proactive authentication reduced multi hop distance by pre- distributing pair-wise master key(PMK), and certificate of-log-in authentication earlier than stirring of a roaming client to a distinct access point. The handoff latency is reduced by ticket-based protocols with the tickets as thriving log-in substantiation. In spite of that, the previous accessible methods involve modifications in original authentication protocols (distinct key architecture, or trust relationships). The other handoff latency method named as security context transfer schemes have been proposed by various researchers [14, 15, 16]. Zhu *et al.* [17] proposed a secure localized authentication and billing scheme for WMNs (SLAB). None of the existing techniques provide guarantee for reduced authentication delay [18] and resiliency against security attacks [19].

Recently, authors [20] used Hyper ledger Fabric (HLF) which is a block chain implementation framework. Hyper ledger projects hosted by the Linux Foundation. Moreover, authors evaluate HLF in a real production mesh network. Aniruddh *et al.* [21] analyze and assess two existing block chain software stacks, named as Hyper ledger Fabric (HLF) and Ethereum geth with Proof of Authority (PoA) intended as a local lightweight distributed ledger, deployed in a real city-wide production mesh network and in laboratory network. The limitation of the aforementioned method is the author evaluates block chain framework HLF and Ethereum geth. They didn't mentioned how to secure data as well as how can be block chain used for reducing authentication delay during hand-off procedure. Rathee et al. [22] proposed an approach for reducing handoff latency and computation cost which is based on diffie-Hellman curve cryptography in WMNs. The limitation of existing method is that diffie- Hellman method used secret sharing key which is not as secure as RSA encryption algorithm. Further, authors [23] proposed a method as symmetric key encryption based approach for reducing handoff latency. In this approach mesh client (MC) authenticate itself to mesh router (MR) by ticket which is generated by authentication server. The strengthen of this approach it will reduce authentication but the limitation of this approach is it will not secured data during handoff.

V. PROBLEM FORMULATION

None of the aforementioned existing techniques [6, 10-19] are able to reduce handoff latency authentication. Moreover, the other limitations of existing approach [6, 10-19] are they are unable to secure data, store data during handoff procedure. Thus the main objective of the proposed approach to reduce handoff authentication delay with secure data transmission under several threats using block chain method.

The proposed method emphasis on tumbling both intra and inter-domain handoff substantiation delay using block chain. As per authors best knowledge block chain used first time in WMN for reducing handoff latency.

VI. PROPOSED APPROACH

Wireless mesh networks (WMNs) have recently materialized to be a lucrative elucidation to carry large-scale wireless Internet access in academics and industry. One of the significant elements of realizing large-scale WMNs is mobility management. Further, a secure and coherent handoff plays a vital role in mobility management. However, research communities have proposed several handoff procedures for WMN with their pros and cons. Every technique have own their attributes as above said in related work. Thus, in this manuscript, we have proposed a block chain technique to reduce handoff authentication latency in WMNs. Further, proposed approach also secure data during handoff. The proposed approach used decentralized block chain. Although, block chain have two types as centralized and decentralized Zheng *et al.* [24] and Kaushik *et al.* [25]. Authors [25] have defined centralized as "Centralization is the consistent and systematic way of entrusting authority to people who are in the centre of the organization" while decentralized can be defined as "decentralized structure is independent of any centralized authority and therefore eliminates the need for a central bank".

The proposed approach based on decentralized structure. Block chain is a sequence of block, which contains the entire information about the mesh client block (MCB) and mesh router block (MRB). Figure 7 shows the proposed approach block chain architecture. Every block summits to the previous block through a allusion that is effectively a hash value of the preceding block titled as parent block. Further, the uncle blocks (children of the block's precursor's) hashes will also be accumulated in ethereum block chain [26]. The genesis block is a first block of block chain because of it has no parent block. Moreover, the proposed method can be explained by considering a scenario. In proposed method, all MRB and MCB are interlinked by block chain according to the rule of block chain every block contains data, hash key, and has key of immediate previous block (parent block). Moreover, they have right to access information of parent block. Let us think about a situation in which there is a plummet in the SNR ratio through which the mobile client requires to abscond its present serving MRB and look for a new foreign mesh router block FMRB. In that case, parent block of roaming client block (RMCB) share roaming client block data with nearest interlinked FMRBs. When a RMCB establish a connection with nearest FMRB then it will re-authenticate itself on the behalf of their hash key which are already shared by parent block with FMRB. Further, RMCB get a new hash key for assessing the services of FMRB. Although, there is another issue comes in light that during handoff how data will be protected in that case data will be encrypted and stored in parent block because of parent block is the nearest block of RMCB.

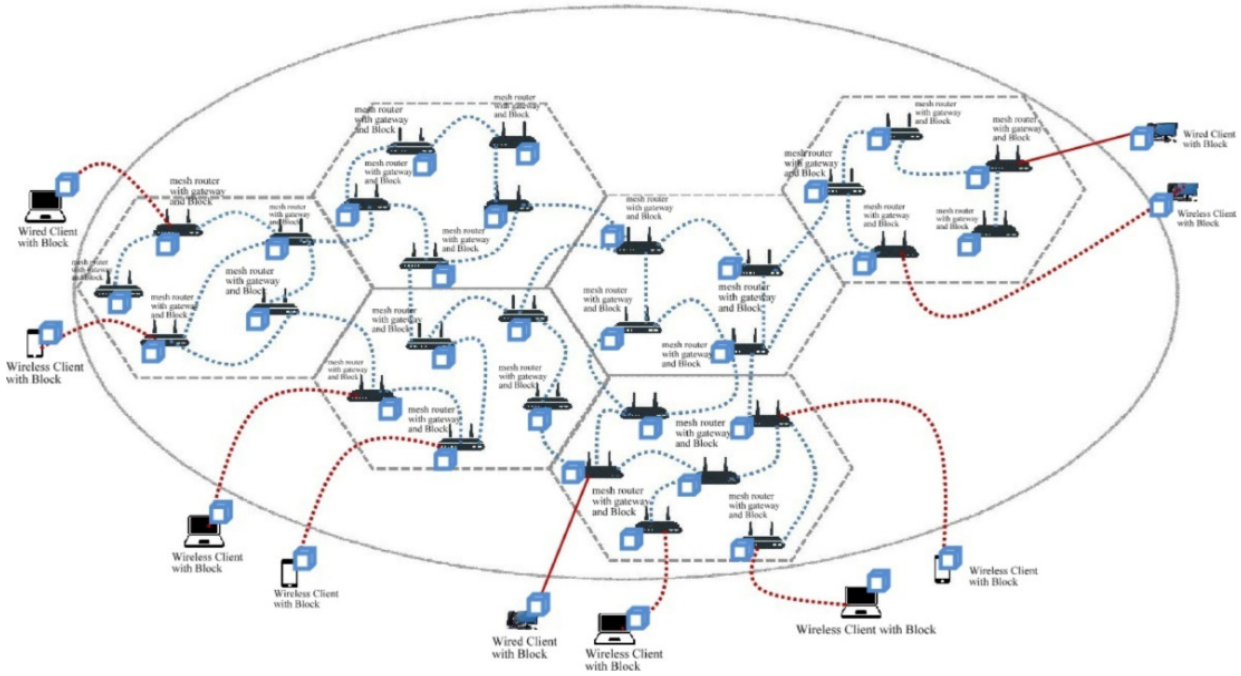

Fig. 7. Proposed block chain based architecture for WMNs.

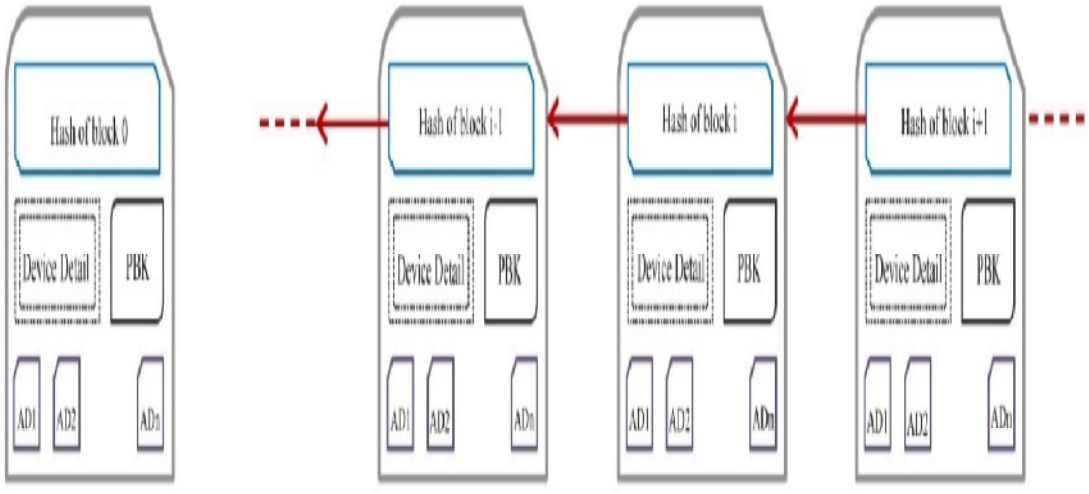

Fig. 8. Proposed block chain sequence for WMNs.

A. Block Chain

A block chain consists of a sequence of blocks which holds entire transaction details [27]. A block comprises of block header which enclosed the subsequent data which are shown in Fig. 8. Authors [27] presents a review on block chain and their characteristics. Although, block header detailed description in terms of wireless mesh network is mentioned below: Fig. 8 and 9 shows the blueprint of block chain and detailed structure of block.

(i) Block version: specify which set of block validation rules to follow.

(ii) Parent block hash: it denotes the prior block's hash value in the 512-bit hash values.

(iii) Merkle tree root hash: it represents the entire block's connections in the form of hash value.

(iv) Device information: It contains MRCB, MCB information.

(v) nBits: current hashing target in compact format.

(vi) Nonce: a 4-byte field, which usually starts with 0 and increases for every hash calculation.

An asymmetric cryptography mechanism is being used in block chain to authenticate the substantiation of transactions NRI [28-29]. Moreover, digital signature relies on asymmetric cryptography which is employed in a hypocritical atmosphere.

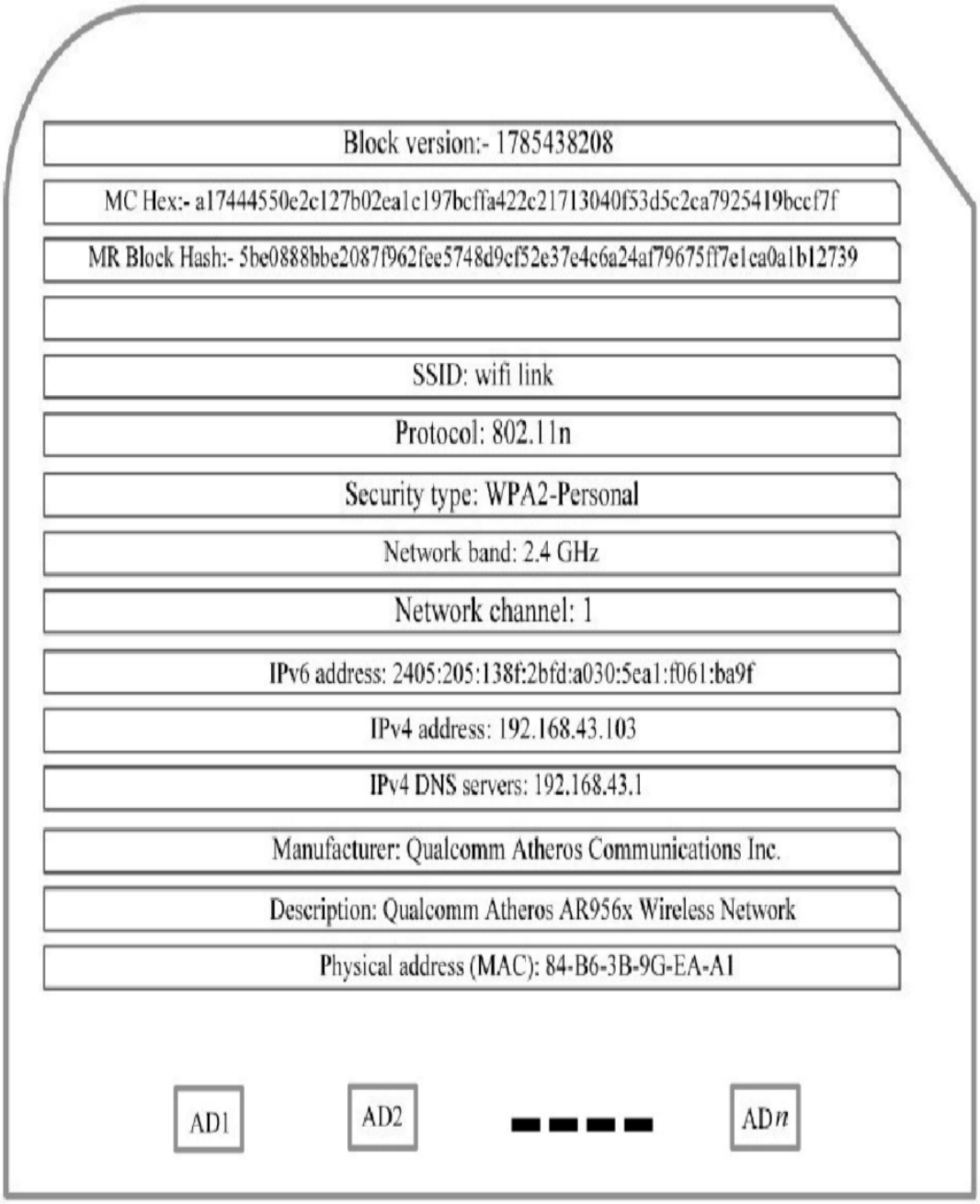

Fig. 9. Proposed block architecture for WMNs.

VII. CONCLUSION AND FUTURE WORK

This paper presents a novel method which is based on block chain technique for reducing handoff authentication delay. Further, the proposed approach also secure data during handoff process. The proposed method authenticates MCB without using third party as authentication server. Moreover, the proposed approach secure data during handoff latency by storing or encrypting data in parent block. The block chain is more secured in comparisons of existing techniques for reducing handoff latency, or securing data because of it will contain parent block hash key through which information shared in a chain manner among the blocks. The block chain used hash key which is used to encrypt data secretly. In future, we implement proposed approach experimentally on block chain framework named as Hyper ledger (open source) tool, network simulator (NS2), and packet tracer. In future, we generate mesh network using HLF tool and after that we used network simulator NS2 for secure packet transmission from MR to MC.

REFERENCES

[1]. Akyildiz, I.F., Wang, X. and Wang, W., (2005). Wireless mesh networks: a survey. *Computer networks*, Vol. **47**(4): 445-487.

[2]. Akyildiz, I.F. and Wang, X., (2005). A survey on wireless mesh networks. *IEEE Communications magazine*, Vol. **43**(9): S23-S30.

[3]. Kozat, U.C., and Tassiulas, L. (2003). "Throughput capacity of random ad hoc networks with infrastructure support". In *Proceedings of the 9th annual international*

conference on Mobile computing and networking, 2003, Page(s) 55-65.
[4]. Jun, J., & Sichitiu, M.L. (2003). The nominal capacity of wireless mesh networks. *IEEE wireless communications*, **10**(5): 8-14.
[5]. Sharma, K., and Shrivastava, G. (2014). Public key infrastructure and trust of Web based knowledge discovery. *Int. J. Eng., Sci. Manage.*, **4**(1): 56-60.
[6]. Xu, L., He, Y., Chen, X. and Huang, X., (2014). Ticket-based handoff authentication for wireless mesh networks. *Computer Networks*, **73**: 185-194.
[7]. Shin, S., Forte, A. G., Rawat, A. S., and Schulzrinne, H. (2004). "Reducing MAC layer handoff latency in IEEE 802.11 wireless LANs". In *Proceedings of the second international workshop on Mobility management & wireless access protocols*, 2004, Page(s) 19-26.
[8]. Ramani, I., and Savage, S. (2005). SyncScan: practical fast handoff for 802.11 infrastructure networks. In *Proceedings IEEE 24th Annual Joint Conference of the IEEE Computer and Communications Societies,* Vol. **1**: 675-684.
[9]. Brik, V., Mishra, A., and Banerjee, S. (2005). "Eliminating handoff latencies in 802.11 WLANs using multiple radios: Applications, experience, and evaluation". In *Proceedings of the 5th ACM SIGCOMM conference on Internet Measurement, 2005, Page(s)* 27-27.
[10]. Duan, X., and Wang, X. (2015). Authentication handover and privacy protection in 5G hetnets using software-defined networking. *IEEE Communications Magazine*, **53**(4), 28-35
[11]. Dalal, R., Khari, M., and Singh, Y. (2012). Authenticity check to provide trusted platform in MANET (ACTP). In *Proceedings of the Second International Conference on Computational Science, Engineering and Information Technology* (pp. 647-655). ACM.
[12]. Forsberg, D., Ohba, Y., Patil, B., Tschofenig, H. and Yegin, A., (2008). Protocol for carrying authentication for network access (PANA). *RFC5191, http://www. ietf. org/rfc/rfc5191. txt.*
[13]. Tseng, Y.M. (2009). USIM-based EAP-TLS authentication protocol for wireless local area networks. *Computer Standards & Interfaces*, Vol. **31**(1): 128-136.
[14]. Loughney, J., Nakhjiri, M., Perkins, C., & Koodli, R. (2005). *Context transfer protocol (CXTP)* (No. RFC 4067).
[15]. Huang, C.M., & Li, J.W. (2009). A cluster-chain-based context transfer mechanism for fast basic service set transition in the centralized wireless LAN architecture. *Wireless Communications and Mobile Computing*, **9**(10): 1387-1401.
[16]. Fu, A., Lan, S., Huang, B., Zhu, Z., and Zhang, Y. (2012). A novel group-based handover authentication scheme with privacy preservation for mobile WiMAX networks. *IEEE Communications Letters*, Vol. **16**(11): 1744-1747.
[17]. Zhu, H., Lin, X., Lu, R., Ho, P.H., & Shen, X. (2008). SLAB: A secure localized authentication and billing scheme for wireless mesh networks. *IEEE Transactions on Wireless Communications*, **7**(10), 3858-3868.
[18]. Li, J., Chen, X., Li, M., Li, J., Lee, P.P., & Lou, W. (2014). Secure deduplication with efficient and reliable convergent key management. *IEEE transactions on parallel and distributed systems*, **25**(6): 1615-1625.
[19]. Pierson, G., & DeHaan, J. (2007). *U.S. Patent No. 7,272,728*. Washington, DC: U.S. Patent and Trademark Office.
[20]. Mennan Selimi, Aniruddh Rao Kabbinale, Anwaar Ali, Leandro Navarro, and Arjuna Sathiaseelan (2018). "Towards blockchain-enabled wireless mesh networks." *In Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems*, ACM, 2018, Page(s): 13-18.
[21]. Kabbinale, A.R., Dimogerontakis, E., Selimi, M., Ali, A., Navarro, L. and Sathiaseelan, A., (2018). Blockchain for economically sustainable wireless mesh networks. *International Journal of Concurrency and Computation Practice and Experience*: 1-18.
[22]. Rathee, G., & Saini, H. (2018). Authentication Through Elliptic Curve Cryptography (ECC) Technique in WMN. *International Journal of Information Security and Privacy (IJISP)*, **12**(1), 42-52.
[23]. Rathee, G., & Saini, H. (2016). A Fast Handoff Technique in Wireless Mesh Network (FHT for WMN). *Procedia Computer Science*, **79**, 722-728.
[24]. Zheng, Z., Xie, S., Dai, H. N., & Wang, H. (2016). Block chain challenges and opportunities: A survey. *Work Pap.–2016*.
[25]. Kaushik, A., Choudhary, A., Ektare, C., Thomas, D., & Akram, S. (2017). Blockchain—Literature survey. In *2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT),* 2017 Page(s): 2145-2148.
[26]. Buterin, V. (2014). A next-generation smart contract and decentralized application platform. *white paper*.
[27]. Zheng, Z., Xie, S., Dai, H., Chen, X. and Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE International Congress on Big Data (BigData Congress),* 2017, Page(s) 557-564.
[28]. NRI: Survey on block chain technologies and related services. Tech. rep. (2015)
[29]. Vishwakarma, R. and Hashiam, M.I., (2015). An Enhancement of Security level under varying Black Hole attacks in Mobile ad-hoc Network. *International Journal of Electrical, Electronics and Computer Engineering*, Vol. **4**(1): 57-65.

How to cite this article: Malik, S. and Kumar, R. (2019). A Novel Block Chain-Based Approach for Secure Handoff in WMN with Reduced Authentication Delay. *International Journal of Emerging Technologies*, **10**(2): 299–306.