IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

SECURITY SOLUTIONS FOR MOBILE AD HOC NETWORKS

[1]Dr. Milindkumar Vinayakrao Sarode

[1] Head of Computer Engineering Department,
[1]Government Polytechnic Nagpur, India.

Abstract: As marked in recent technical inventions, the initiation of the Mobile Ad-hoc Networks has steered to momentous growth in the field of engineering and technology. Today, the world has seen the extensive acceptance of IP-based networking. This technological development is bringing about substantial radical changes, suggesting the Mobile Ad-hoc Networks as transformative as the industrial revolution. There are many challenges in the overall security and privacy aspects of the Mobile Ad-hoc Networks. Reliability problem is also a wireless link characteristic due to limited wireless transmission. Due to the broadcast of wireless medium packets loss and errors in the data occur. In comparison to the wired network the wireless networks are more vulnerable to security threats.

Index Terms **- block chain, Security, mobile ad-hoc network (MANET).**

Introduction

Present-day trend shows that Mobile Ad-hoc Networks is playing a important role in human lives, and it will continue to unveil new, brilliant, scientific and technological breakthroughs embedded in the capability of smart devices and applications that are connected to the internet. Block chain technology is growing speedily due to its distributed, secure, and see-through nature which makes information and privacy breaks difficult and practically technically impossible. Succeeding sections of the paper are structured as follows: Section II gives an overview and definition of block chain. Section III provides a conceptual overview and definition of the Ad-hoc Mobile network and associated issues. Section IV discusses subsidiarity and immutability features of block chain and how they could help to mitigate the security challenges in Ad-hoc networks solutions. Section V concludes the paper.

BLOCK CHAIN OVERVIEW AND DEFINATION

A block chain is a distributed and public digital record that is used to record communications across various computers so that the record cannot be altered without the alteration of all subsequent blocks and the consent of the network. A block chain gathers information together in sets, known as blocks that hold sets of information. Blocks have certain storage capacities and when filled are closed and linked to the previously filled block, forming a chain of data known as the block chain. All new information that follows that freshly added block is compiled into a newly formed block that will then also be added to the chain once filled. The idea of block chain was theorized in 2008. Today, block chain has evolved into one of the modern-day major inventions and has found its way into many applications beyond crypto currencies, casing several fields with financial services, transportation, e-commerce, manufacturing, and so many. Block chain technology realizes distributed security and trust in several ways. To begin with, new blocks are always stored linearly and chronologically. That is, they are always added to the "end" of the block chain. After a block has been added to the end of the block chain, it is very difficult to go back and modify the contents of the block unless a majority of the network has reached a consensus to do so. Thus each block contains its own hash, along with the hash of the block before it, as well as the previously mentioned timestamp. Hash codes are created by a mathematical function that turns digital information into a string of numbers and letters. If that information is edited in any way, then the hash code changes. Presently, so many projects are implementing block chains in a variety of ways to help society other than just recording transactions—for example, as a way to vote securely in democratic elections. The nature of block chain's that fraudulent voting would become far more difficult to occur. For example, a voting system could work such that each citizen of a country would be issued a single crypto currency or token. Each candidate would then be given a specific wallet address, and the voters would send their token or crypto to the address of whichever candidate for whom they wish to vote. The transparent and traceable nature of block chain would eliminate both the need for human vote counting and the ability of bad actors to tamper with physical ballots. The number of live block chains is growing every day at an ever-increasing pace. As of 2022, there are more than 10,000 active crypto currencies based on block chain, with several hundred more non-crypto currency block chains. A public block chain, also known as an open or permission less block chain, is one where anybody can join the network freely and establish a node. Because of their open nature, these block chains must be secured with cryptography and a consensus system like proof of work. A private or permissioned block chain, on the other hand, requires each node to be approved before joining. Because nodes are considered to be trusted, the layers of security do not need to be as robust. A block chain platform allows users and developers to generate novel uses on top of an existing block chain structure.

I. AD-HOC NETWORK - OVERVIEW, DEFINITION, APPLICATIONS, AND ISSUES

Usually, all the networks are having fixed network infrastructure with centralized administration which requires for their operation, potentially consuming a lot of time and money for set-up and maintenance. Additionally, an increasing number of devices such as laptops, personal digital assistants (PDAs), pocket PCs, tablet PCs, smart phones, MP3 players, digital cameras, etc. are provided with short-range wireless interfaces. In addition, these devices are getting smaller, cheaper, more user friendly and more powerful. This evolution is driving a new alternative way for mobile communication, in which mobile devices form a self-creating, self-organizing and self-administering wireless network, called a mobile ad hoc network. Contrasting to infrastructure wireless networks, where each user directly communicates with an access point, a mobile ad hoc network, or MANET, does not rely on a fixed infrastructure for its operation. Mobile ad hoc networks are projected to become an important part of the future 5G architecture, which aims to provide universal computer environments that support users in achieving their tasks, retrieving information and communicating anytime, anywhere and from any device. The concept of mobile ad hoc networking is not a new one. The advantages of ad-hoc networks such as flexibility, mobility, Flexibility and independence of fixed infrastructure, triggered immediate interest among military, police and rescue agencies in the use of such networks under disorganized or hostile environments. Currently, mobile ad hoc network research is a very vivacious and active field and the efforts of the research community, together with current and future MANET enabling radio technologies will certainly pave the way for commercially viable MANETs and their new and exciting applications, with some of these commercially oriented solutions already starting to appear self-administering capabilities, ad hoc networks can be rapidly deployed with minimum user intervention. There is no need for detailed planning of base station installation or wiring. Also, ad hoc networks do not need to operate in a stand-alone fashion, but can be attached to the Internet, thereby integrating many different devices and making their services available to other users. Furthermore, capacity, range and energy arguments promote their use in tandem with existing cellular infrastructures as they can extend coverage and interconnectivity.

3.1Techological Challenges

The specific characteristics of MANETs enforce many challenges to network protocol designs on all layers of the protocol stack5. The physical layer must deal with rapid changes in link characteristics. The media access control (MAC) layer needs to allow fair channel access, minimize packet collisions and deal with hidden and exposed terminals. At the network layer, nodes need to cooperate to calculate paths. The transport layer must be capable of handling packet loss and delay characteristics that are very different from wired networks. Applications should be able to handle possible disconnections and reconnections. Furthermore, all network protocol developments need to integrate smoothly with traditional networks and take into account possible security problems.

II. BLOCKCHAIN – A PRACTICAL SOLUTION TO THE AD-HOC NETWORK SECURITY THREATS

Block chain has the potential to remove ad hoc network security concerns in various ways given that it offers a profoundly different model for storing and managing information on the internet. The distributed nature of block chain technology has the ability to deny any sort of central attack which could lead to the compromise of the entire network. In a distributed system, there is no governing authority looking after the network, but as an alternative, a group of nodes maintains the network, making it distributed. In a block chain system, data is stored on various nodes. Before adding or removing any data on the network, all participating nodes must approve and verify it. This approval process helps to remove the single point of failure. Culprits of malicious activities would have to target individual nodes on the network to breach the network security. Using a block chain system or network makes it possible for smart devices to actively participate in the validation process. This means the network would be able to protect against any break or security compromise by validating predetermined satisfactory behaviour for any anomalies. The devolution feature of block chain technology helps to ensure no change is allowed on a network without a shared agreement from all the network participants. Once a device on the network is identified as not behaving correctly or as it should, it can be readily isolated to prevent it from being used to gain further access to sensitive information. Unlike centralised systems where hackers can target and intercept the information sent between a server and a device, there is no single server or gateway in decentralised systems, meaning that the possibility of a man in the middle attack is allayed. Immutability is another definitive property of block chain-based systems which promotes transparency and ensures that system resources or data cannot be altered or corrupted. This feature has the potential to incorporate a quick, cost effective and efficient examining process, and bring more trust and integrity to the data shared or stored on the internet. In block chain systems, each transaction that is verified and validated by the participants on a network is time stamped and embedded into a 'block' of information, cryptographically secured by a hashing process that connects to and integrates the hash of the previous block, joining the chain as the subsequent chronological update. The hashing process of a new block always incorporates a set of data from the previous block's hash output. This connection in the hashing process makes the chain incorruptible i.e., it is not feasible to alter or delete data after it has been verified, validated, and placed in the block chain. If attempted, the subsequent blocks in the chain would reject the attempted tampering. Altogether, a critical examination of some key features of block chain as highlighted above suggests it is a technology that can appreciably improve the security aspects of IoT systems, albeit, it has its own drawbacks like every other emerging invention. While the prospects of merging blockchain with IoT for enhanced security sounds like a match made in heaven, the idea of combining the two technologies is still maturing and requires careful consideration, to achieve a viable outcome. Today, trends within the industry suggest that the adoption of blockchain solutions by mainstream sectors (such as, financial institutions, insurance, supply chain, government) is gaining momentum and the qualities of blockchain technology makes it one of the most revolutionary tools of the contemporary era that can complement the security aspect of IoT systems.

explained above suggests, it is a technology that can noticeably improve the security aspects of ad-hoc network systems

III. CONCLUSION

The quick evolution in the field of mobile computing is pouring a new unusual way for mobile communication, in which mobile devices form a self-creating, self-organizing and self-administering wireless network, called a mobile ad hoc network. Its inherent flexibility, lack of infrastructure, ease of arrangement, auto-configuration, low cost and budding applications make it an essential part of future universal computing environments. the unified incorporation of mobile ad hoc networks with other wireless networks and fixed infrastructures will be an essential part of the growth towards future fifth generation communication networks. From a technological point of view, the understanding of this vision still requires a large number of challenges to be solved related to devices, protocols, applications and services.

REFERENCES

[1] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt and Piet Demeester, An Overview of Mobile Ad Hoc Networks: Applications and Challenges.

[2] Nsima Udoh, Blockchain: A Security Solution for the IoT?. International Journal of Future Computer and Communication, Vol. 11, No. 1, March 2022, pp. 1-6.

[3] S. Haber and W. S. Stornetta, “How to time-stamp a digital document,” Journal of Cryptography, 1991, vo. 3, pp. 99-111.

[4] Chlamtac, I., Conti, M., and Liu, J. J.-N. Mobile ad hoc networking: imperatives and challenges. Ad Hoc Networks, 1(1), 2003, pp. 13–64.

[5] Royer, E., and Toh, C. A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks. IEEE Personal Communications, 6(2), Apr. 1999, pp. 46–55.

[6] Royer, E., and Toh, C. A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks. IEEE Personal Communications, 6(2), Apr. 1999, pp. 46–55.

[7] Dr.S.S.Dhenakaran and Dr.S.S.Dhenakaran, “An Overview of Routing Protocols in Mobile Ad-Hoc Network”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 2, pp. 251-259, February 2013.

[8] V. Saravanan Asst and D.Vijayakumar, “Performance Of Reactive And Proactive MANET Routing Protocols With Trajectories”, International Journal of Engineering Research and Technology (IJERT), Volume 1, Issue 8, pp. 1-11, October 2012

[9] S. Mueller, R. P. Tsang, and D. Ghosal, “Multipath routing in mobile ad hoc networks: Issues and challenges,” Performance Tools and Applications to Networked Systems, pp. 209–234, 2004.

[10] D. Wang, M. Hu, and H. Zhi, “A survey of secure routing in ad hoc networks,” The Ninth International Conference on Web-Age Information, pp. 482–486, 2008.