IMPLEMENTING BLOCK CHAIN SECURITY TO PREVENT DDOS ATTACKS IN NETWORKS

Ashu¹, Rashima Mahajan² and Sherin Zafar³

¹*ECE, MRIIRS, Faridabad, India*

²*CSE, FET, MRIIRS, Faridabad, India*

³*CSE, SEST, Jamia Hamdard, New Delhi, India Country*

¹ashuone@gmail.com, ²rashima.fet@mriu.edu.in, ³zafarsherin@gmail.com

Abstract— identifying attacks on networks is an arduous task. IOT (Internet of Things) based Mobile Ad-hoc Networks (MANETs) are networks in which mobiles organize themselves in dynamic topology deprived of any centralized system. MANETS can be treated as a category of Wireless Mesh Networks (WMN). The rate of attacks any network faces just doubles itself with a distributed environment. The proposed approach in this paper utilizes Block Chain approach as a force for prevention of DDOS attack (Distributed Denial of Service). The proposed methodology will be a boom for various businesses and industries for prevention and mitigation of DDOS attack. Since block-chain is a decentralized system having multiple nodes it will ensure that attacks are not concentrated on a single centralized source. An attacker will have to gain access to various multiple nodes simultaneously making it difficult, expensive and time-consuming to implement an attack. The blockchain methodology will create decentralized network of servers that will send bandwidth in a flash to the servers that are facing attacks. DDOS attacked server will absorb excess traffic by utilizing additional bandwidth. The approach posits a block chain algorithm for securely sharing IOT based datasets to ensure integrity of shared datasets across infra-structure less WMN.

Keywords— DDOS attack; Block Chain Algorithm; IOT; MANET; WMN; HWMP

1. INTRODUCTION

Due to the rapid development and continues improvement, wireless networks has been mounting from low level task of information transmission to wide-ranging service for innumerable network based dealings. The absence of central infrastructure makes wireless networks to work in ad hoc mode, because of which network can reconfigure itself on leaving or joining of the node. When mobile replace those nodes of network than the network is known as MANET (Mobile ad hoc Network). MANET being robust in nature can be considered as type of wireless mesh networks (WMN). The various characteristics of WMN which make them robust are: Self-configuration: it indicates the ability of the network to incorporate any fresh node in to the prevailing arrangements of network, deprived of the intervention of the any supervisor. Self-Healing: this helps to discover the best possible shortest and trustworthy and route in network, even if the nodes participating in the network lose their signal or are blocked by some means. Wireless mesh arrangements permit confined networks to route more rapidly, as confined packets need not to stretch back to a principal server. Adaptable: because of easy installation and

Received: September 16, 2019
Reviewed: November 18, 2019
Accepted: December 4, 2019

uninstallation of network nodes and expandable as per the less or more coverage requirements [1].

1.1 WIRELESS MESH NETWORK

WMN are considered not only as self-organized but also as self-configured network, since various devices acting as nodes along with the networks communicate in a mesh topology, to be responsible for connectivity [2]. WMN comprehends nodes which are further interconnected via means of wireless technology for communication. These mesh nodes are normally named as clients for example laptop, mobile phones along with routers, containing Wi-Fi admittance sockets. It possess distributed architecture as shown in the figure 1 below different clients in addition to routers connect to distribute the association [2, 3]. The key features and pluses of WMNs in delivering network facilities for instance Internet access, transferring information through video and voice and transmitting data among networks are: Coverage, Compatibility, Mobility, Heterogeneity and Scalability. Therefore WMN turns to be a prominent communication innovation in modern time, which embraces multi-hop progressing procedures for speedy information correspondence with least loss of data. It's rising as an extremely developed communication technology also appropriately designed for numerous cyber-physical alliance applications like in smart grids, applications related to defense and for system based on internet of things[4]. WMN is susceptible to a number of attacks categorized as DDOS; such as flooding, black-hole and grey-hole because of its multi- hop nature. The repeated broadcast of large quantities comprising HELLO packets, information and unwanted information through the mischievous node is known as flooding attack leading to denial of service. Due to this jamming is caused at the receiver and further at communication stations of the network, leading to upsurge of packet dropping ratio, ultimately blocking the communication. Because of these WMN's apposite for numerous applications in military as well as in civilian arenas. WMN gives the best possible solution in various domains where wired communication cannot be done or is dangerous, such as in public safety and in wireless communication system intend for disaster recovery, thus WMN is a new suitable solution as it deals with easy and quick connectivity over a wireless technology acting as an intermediate.

Fig. 1 Wireless mesh network.

1.2 DDOS ATTACKS IN WMN

WMNs are extremely susceptible to numerous categories of existing attacks because of their intermediate medium which is common wireless access and constrained assets. The intended users are not able to make use of network resources or infrastructure in presence of attacks such as denial of service. Since the WMN runs on unlicensed 2.4GHz band, attacker (to prevent the service from its functioning efficiently, temporally or indefinitely). To reduce network resources by means of directing a torrent of packets from malicious node (clients and routers) whose number could be one or more, is the main objective of DDOS attack. Ultimately cause congestion in the network by injecting huge amount of traffic into the network. These types of attacks could be found in all the layers (Physical Layer, Link layer, Network Layer, Transportation Layer) of WMN. Disseminated refusal of administration i.e. DDOS assaults can cut down your site and abandon you difficult to reach to the remainder of the web for a considerable length of time or days on end. Getting the pieces after a DDOS assault is a long and exorbitant procedure. The normal money related expense of a DDOS assault for a little or moderate size business is about \$123,000, and that number is on the ascent. DDOS assaults have become greater and progressively complex throughout the years, and they save no site or system. Thirty-three per cent of organizations were hit by DDOS assaults in 2017, about twofold the quantity of assaults in 2016. Eight-two per cent of associations have confronted various DDOS assaults [5, 6].

Routing disruption along with resource depletion, are the attacks which can be present in protocols of network routing and are thoughtful concern in a mesh based network as they can confess not only reliability of the paths, but also the accessibility of the complete network. Mischievous nodes possibly can create mischievous traffic, interrupt as well as alter packets, or refuse to forward packets simply by dropping them. In presence of even protection such as end-to-end cryptographic solution, a nasty node can descent packets going through it, or influence the network paths by issuing fake routing information. Many routing protocols have been proposed by the researcher groups. However there is a serious demand to study the performance features of the routing protocol in WMN's. This paper delivers a comparison of performance metrics of AODV (reactive) and HWMP (hybrid).

1.3 HWMP

The proposed approach explicitly emphasis on HWMP being the compulsory protocol for routing intended to IEEE 802.11s built mesh topology based networks. HWMP is a hybrid wireless mesh protocol [3] functional at layer-two and for route select utilizes MAC addresses. Since it conglomerates together reactive and pro-active routing approaches, hence is known as hybrid protocol. The amalgamation of reactive features with the proactive features of HWMP permits competent route selection for wide-ranging diversity of mesh based networks. HWMP offers tasks in two modes one on demand and second proactive. Two modes are used simultaneously, as in reality the proactive mode is basically an extension of the on-demand mode. For discovering the route selection process HWMP utilize four imperative information elements (IEs) out of which three IE (Path Request (PREQ), Path Reply (PREP) and Root Announcement (RANN))are employed in routes selection process, and the fourth one Path Error (PERR) is cast-off for route-maintenance.

In case of HWMP, route to the destination is going to be defined by the subsequent hop at each in-between mesh station (written as mesh STA). PREQ is broadcasted whenever a path discovery is to be beginning i.e. source needs to direct data to a target for same the route is to be discovered. For route selection process, from present PREQ Information Element three sub field: Hop Count, Element TTL, Metric and the Target-Only in Per Target field are activated by the intermediary nodes. The hop-count is

operated by every single intermediate node alongside the particular route. The assessment for same is set to a numeral equivalent to the quantity of jumps from the initiator STA to the mesh STA conveying the PREQ. Component TTL shows the amount of hops allowable for the PREQ component and is chiefly used to avoid the PREQ element from crossing the network infinitely. It is for the most part used to keep the PREQ component from crossing the system unendingly. At first, the estimation of TTL component set to a number equivalent to diameter of mesh network. The metric field is fixed for accumulative measurement from the initiator to the mesh STA communicating the PREQ. The IEEE 802.11s states the practice of air-time link metric (ATLM) as standard link metric to detect a capable radio route. Everything aforesaid conversed turfs are improved by the in-between nodes consequently, empowering improved route selection.

This section throws an insight on MANET, wireless mesh networks along with HWMP and the challenges faced in form of attacks. Further security in networks is sorted according to the reactive and proactive approaches. Gaps in study that lead to problem formulation are detailed in Section 2. The concept of Block chain, widely employed in transactions in public ledger along with the mathematics lying at backend of block chain concept is described in Section 3, emphasizing the potential of block chain in tackling the security issues. Section 4 elaborates securing attack condition in proposed HWMP protocol via block chain and is compared with the conventional AODV approach. Hop counts and response delay are the selected indicators. Section 5 provides the simulation analysis of the proposed approach that validates the proposed approach. Section 6 concludes the paper through Discussions and Conclusion followed by references in the end delivers a comparison of performance metrics of AODV (reactive) and HWMP (hybrid).

2. GAPS IN STUDY AND PROBLEM FORMULATION

Studies carried on WMN for detection of DDOS attacks could be categorized as protocol improvement and their comparison becomes the basis of the proposed work. How block-chain has become the most trustworthy approach of various fields is also highlighted in this discussion through various related works. The research analysis below presents various gaps in study and problem formulation of the proposed study:

1. Research studies highlight that DDOS type attacks cause serious damage on the performance of any network and should be strictly prevented. So detection of malicious node in the IOT- MANET based network is the prime-most concern of the proposed study.
2. It is too difficult to identify the destructive nodes along the network. The aim of the proposed algorithm is to identify the destructive node accordance to the behavior of nodes in the system by adopting block chain mechanism.
3. Network suffering from attacks face drawbacks; less throughput; low packet delivery ratio; high network routing overhead etc. Network small in structure is more vulnerable for these types of attacks and consequently drawbacks. Proposed algorithm focuses to offer more security and stability in a Wireless Mesh Networks i.e. to develop efficient security mechanism and secure routing methodologies against different attacks.
4. In the digital world today various secure mechanism are not able to distinguish and track various malicious attacks that occur in the system. The proposed approach works on the problem to distinguish distributed flood attack traffic from flash crowd.
5. Various investigations need strong usage and reenactment modules for a wide range of assaults to be utilized in testing and assessing new proposed

arrangements. The proposed methodology giving such a structure that will assist specialists with providing handy arrangements. Reproduction configuration prompts a brilliant discovery component that uses square chain way to recognize and secludes noxious hubs in progressing WMN.

6. Businesses are starting to investigate block-chain to counteract and relieve DDoS assaults. Block-chain is a decentralized framework with different hubs. Working the DNS on a block-chain would guarantee that assaults are not focused on a brought together source, devastating it. To effectively cut down a DNS on a block-chain, programmers would need to access numerous hubs in the meantime, which makes executing the assault progressively troublesome, tedious, and costly. On the other hand, organizations are additionally utilizing block-chain innovation to make a decentralized system of servers that can rapidly send transmission capacity to different servers confronting assaults. The assaulted server would then be able to withstand the DDoS surge by engrossing the abundance traffic utilizing the extra transfer speed.

3. SECURITY VIA- BLOCK CHAIN

Security and privacy of the systems, along with its computations is critical in data-sensitive applications. Figure 2 explain the classifications of the security techniques carried by different researchers. Broadly the security threats can be differentiated on the bases of Reactive approaches and Proactive approaches. Reactive methods are further regarded as:

A) Systems based on Intrusion Detection (ID) only and systems based on Intrusion Prevention (IP)

B) Collaborative security approaches.

Furthermost existing A) methods are intended to spot unauthorized admittance challenges and DDOS attacks and can be grouped by the following three different ways: Grouping by approaches, by network structure and by applications [6]. In recent times owed to probability in detecting and preventing a wide variety of attacks, lot of attention is given in a collaborative security paradigm, and could be categorized by network structures, by applications [7,8,9].

Fig. 2 Security Classifications

Block chain can be useful to improve security in networks. It was initially used for maintaining records while doing financial dealings, where transactions are encrypted and lies with all participants; bit coin is one such example. Therefore the transactions are clear and all the alterations can be effortlessly outlined and identified. Fig.3 clarifies a distinctive block chain progression. If transaction occurs, a block is created. The block is announced to all participated nodes of the mesh network. Authentication of new created block is done by one of nodes (termed mining in bit coin) and announced it back. The already exiting nodes/devices will add the new node to their chain of blocks if it's validated and the block properly mentions the preceding node/block[23].

Fig. 3 Block chain Work flow

This concept is enabled by "Block chain" technology. The nodes/blocks participating in the network enter the data and authorize their receipt through elliptic curve digital signature algorithm (ECDSA), which is the behindhand mathematics lying in block chain.

The elliptic curve is a mathematical equation for example $y^2 = x^3 + ax + b$. in most of applications, $a = 0$ and $b = 7$, so above equation reduces to $y^2 = x^3 + 7$.

Elliptic curves have many remarkable thing, for example the feature of non-vertical line traversing 2 non-tangent facts will each time traverse a 3rd point on curve. Certainly, it's a fact that can be discuss that the "addition" on curve as outcome that third point consequential to two specified points. Fundamentally this is implemented in ECDSA, aside from that the processes are performed modulo about large prime number P . Precisely, in ECDSA, addition of two points $(k1, k2)$ and $(l1, l2)$ respectively, and the doubling of $(k1, k2)$, are achieved as per following steps: Addition of $(k1, k2)$ and $(l1, l2)$ is given by the following equations:

$$c = (l2 - k2) / (l1 - k1) \mod M \quad (1)$$

$$r1 = c^2 - k1 - l1 \mod M \quad (2)$$

$$r2 = c(k1 - r1) - k2 \mod M \quad (3)$$

Doubling up of $(p1, p2)$ is represented through following given equations:

$$c = (3k1^2) / 2k2 \mod M \quad (4)$$

$$r1 = c^2 - 2k \quad (5)$$

$$r2 = c(k1 - r1) - k2 \quad (6)$$

“Multiply” processes are classically done by the binary algorithm for multiplication, which are easily amended to ECDSA. To compute $r = n * b \bmod P$, First, choose a modulus P , “base point” $(k1, k2)$, also private key $k1$ (integer between 1 and $P-1$). These two are selected in a way that the base point order (i.e. the maximum amount of times $(k1, k2)$ can be added to itself in advance the addition formula above fails due to zero divide) is prime and at least as large as P (though not required but is generally done, and because of this assumption below algorithm becomes much simple to understand). The process digital signature of data is constructed as follows [10, 11, 12,24].

1. Select some integer $y2$ between 1 and $n-1$, where n is the order.
2. Calculate $(s1,s2) = y2 * (k1,k2)$. If $s1 = 0$, return to step 1.
3. Calculate $s2 = (z1 + s1 * y1) / y2 \bmod n$. If $s2 = 0$, return to step 1.

Obtained digital signature is $(s1, s2)$. Now test the digital signature, as a third party to verify that the transaction is valid. This is finished by the following procedure:

1. Compute: variable $v1 = s2-1 \bmod n$
2. Compute: variable $v2 = z1 * v1 \bmod n$
3. Compute: variable $v3 = s1 * v1 \bmod n$
4. Compute: $(t1,t2) = v2 * (k1,k2) + v3 * (r1,r2)$
5. Validate: $t1 = s1$.

4. PROPOSED METHODOLOGY

Reenactment of the proposed convention contrasting and the ordinary secure AODV approach is done through NS2 by thinking about the accompanying assault circumstance: Since, the DDOS assault decreases the span of courses (or jump tallies) the properties influenced by this specific adjustment can be utilized as a sign of assault thus, in proposed system the bounce checks (hop counts) and the reaction deferral (response delay) can be taken as pointers as talked about beneath:

Step 1: Each hub figures the normal jump (hop count) checks and the fluctuation (variance) of the considerable number of courses in its directing table and updates constantly on entry of new courses (routes).

Let

HopCount_avg: Average hop counts

HopCount_var: Fluctuation of hop counts

HopCount_RREP: Hop counts of the current RREP.

Step2: As of now talked about, that the jump means the assaulted course (attacked route) will be not exactly ordinary thus, first estimation of the likelihood of the present course (of which RREP is gotten) is done enduring an onslaught condition utilizing the accompanying articulations:

```
if (HopCount_RREP > HopCount_avg ){
    Prob_attack=0;
}else{
    if(HopCount_RREP > (HopCount_avg-HopCount_var )){
        Prob_attack=(1-(HopCount_RREP)/(HopCount_avg ));
    }else{
```



```
Prob_attack=1;  
}  
}
```

Step 3: The above calculated Prob_attack indicates possibility that the route is under an attack (assault), but doesn't identifies the attacker hence, for that a block chain mechanism i.e. Block Chain Algorithm to Mitigate DDOS attacks in Wireless Mesh Networks" is proposed

(a)

(b)

Fig. 4 (a) Nodes movement in HWMP Protocol (b) Simulation of HWMP Protocol with Packets being dropped in DDOS attack

Step 4: The block chain based component fills in as, each hub which advances the RREP makes a mark of the parcel information toward the finish of the bundle (for that the RREP parcel design is changed to give space to block chain signature stockpiling of 8 bits for each hub). Consequently, when a hub gets RREP, it right off the bat ascertains the Prob_attack and based on its esteem it applies the mark testing as pursues

p =Random number between 0 to 1 generated by uniformly distributed number generator

```
if( $p < \text{Prob\_attack}$  ){
  if(CheckSignature(RREP)=Fail){
    List the Previous Node as Attacker;
  }else{
    List the Previous Node as Normal;
  }
}
else{
  Ignore Signature Check;
}
```

The advantage of the block chain based system is that it reduces the computational cost of testing the block signatures of all RREP which consequently reduces the energy consumption of nodes also. Figure.4 (a) and (b) shows snapshots of NS2 simulations in normal mode and attack mode consequently and figure.4 (c) depicts the analysis of performance parameters through NS2 visual trace analyzer in attack condition.

Fig. 4 (c) Performance Analysis of Proposed Approach through NS2 Visual Trace Analyzer

5. SIMULATION ANALYSIS

The parameters taken for "Block Chain Algorithm to Mitigate DDOS attacks in Wireless Mesh Networks" with simulation time of 3000s and number of created packets as 160 is listed in Table II below:

Table I. Simulation Parameters for the Proposed Approach

Parameter	Value
Type of Channel	Wireless Channel
Radio-Propagation	Two Ray Ground
Type of Network Interface	Wireless Phy
Type of MAC	Mac-802_11
Type of Interface Queue	Queue: Drop Tail: Pri Queue
Model of Antenna	Omni Antenna
Mobile Nodes	50, 60, 70, 80, 90, 100
Topography Dimensions: X	200m
Topography Dimensions: Y	200m

Conventional AODV and proposed block-chain based HWMP is simulated by NS tool under various levels of attacks depicted through Tables II and III. When there is a DDOS attack delay in a WMN gets even lower as the pernicious (malicious) hub present in the system claims to have a substantial course (valid route) to the goal without checking in the steering table, in this way course revelation process (route discovery process) takes shorter time. With number of hubs as the correlation parameter, when assault level is expanded normal postponement of the proposed verified methodology is kept up. The advantage of proposed block chain based secured approach is that; it decreases the computational expense of testing the marks of all RREP which diminishes the vitality

utilization moreover. Security of the proposed block chain technique is very viable from the customary methodologies as average delay is maintained to provide enhanced security solution for WMN. NS2 a highly recommended simulator has been utilized for verification and validation of the results of the proposed Block Chain Algorithm to Mitigate DDOS attack condition. The importance of the "Block Chain Algorithm to Mitigate DDOS attacks in Wireless Mesh Networks" has been legitimized by re-enacting it under state of assault (which is in all respects improbable to happen with a block chain approach), uncovering compelling outcomes. With number of hubs as the examination parameter, when assault level is expanded normal postponement doesn't drops off and is kept up.

Table II. Simulation Results Depicting Traditional AODV Approach at various Attack levels

S.No	Parameters	Normal Case : Without Attack	AODV Level of Attack: 5%	AODV Level of Attack: 10%	AODV Level of Attack: 15%	AODV Level of Attack: 20%	AODV Level of Attack: 25%)	AODV Level of Attack: 30%
1.	Time of Simulation(s)	3000	3000	3000	3000	3000	3000	3000
2.	Packets being Created	160	160	160	160	160	160	160
3.	Packets being Delivered	142	56	54	53	54	50	51
5.	Average Delay (b/s)	201.34	1.2	2.24	3.3	4.81	6.8	10.1

Table III. Simulation Results of Proposed Block Chain Algorithm to Mitigate DDOS attacks in Wireless Mesh Networks

S.No	Parameters	Normal Case: Without Attack	Proposed Block-Chain Paradigm Level of Attack: 5%	Proposed Block-Chain Paradigm Level of Attack: 10%	Proposed Block-Chain Paradigm Level of Attack: 15%	Proposed Block-Chain Paradigm Level of Attack: 20%	Proposed Block-Chain Paradigm Level of Attack: 25%)	Proposed Block-Chain Paradigm Level of Attack: 30%
1.	Simulation Time (s)	3000	3000	3000	3000	3000	3000	3000
2.	Packets being Created	160	160	160	160	160	160	160
3.	Packets being Delivered	142	58	60	59	53	59	62
5.	Average Delay (b/s)	201.34	1.98	2.9	4.2	5.11	7.9	11.43

Fig. 5 Comparison of Average Delay of Conventional and Proposed Secured Approaches under DDOS Attack

6. CONCLUSION AND FUTURE DIRECTION

The security part of the WMN using HWMP involves a position of extraordinary significance particularly after the developments of different changes and the ascending of new applications. Block-chain is another innovation committed to the information sharing. The latest DDOS assaults have been seen to seize associated gadgets, for example, webcams, infant telephones, switches, vacuum robots, and so forth to dispatch their assaults. The quantity of gadgets remotely controllable through applications is developing exponentially and the Internet of Things (IOT) is relied upon to effortlessly outperform 20 billion associated gadgets before the finish of 2020. One of the related issues is that a large number of the associated gadgets are badly outfitted with safety efforts to anticipate vindictive and inappropriate utilization, and hence end up being the ideal, clueless assets to be enrolled into a botnet. The absence of legitimate security highlights for associated IOT gadgets is chiefly determined by inadequate prioritization on the grounds that the potential for interruption has been disparaged previously, and fabricating expenses and benefit potential manage include choice. So, ongoing occasions may trigger a reexamine to incorporate and advance security includes as a feature of a top notch situating for associated items. At present, tainting gadgets for making a botnet couldn't be simpler for a skillful programmer. Block-chain innovation could empower the making of IOT systems that are peer-to-peer (P2P) and trustless; a setting which evacuates the requirement for gadgets to confide in one another and with no brought together, single purpose of failure. A Block-chain, being an all-around appropriated record, guarantees the security of all exchanges through the cryptographic work of specific members called hubs which approve those exchanges, as a byproduct of remunerations as digital forms of money, for example, Bit coin. This expels the requirement for a focal specialist to verify a gadget to interface with another gadget and furthermore validate a client to login to a gadget.

REFERENCES

- [1] Ms. Sanam E Anto, Ms.S Seetha, Robin K Kuriakose (2012) "A survey on DoS attacks and detection schemes in wireless mesh Networks." International Conference on modeling and optimization and computing 38: 2329 – 2336.
- [2] Li Qiong and Yang Jun (2012) "An Improved AODV Routing Protocol of Wireless Sensor Network" International Conference on Image Analysis and Signal Processing.
- [3] Adnan Ahmed, Kamalrulnizam Abu Bakar, Muhammad Ibrahim Channa, Khalid Haseeb and Abdul Waheed Khan (2015) "TERP: A Trust and Energy Aware Routing Protocol for Wireless Sensor Network IEEE Sensors Journal."15(12).

- [4] Adnan Ahmed, Kamalrulnizam Abu Bakar, Muhammad Ibrahim Channa, Abdul Waheed Khan (2016) "A Secure Routing Protocol with Trust and Energy Awareness for Wireless Sensor Network" , in The journal Mobile Networks and Applications .21(2), pp 272–285
- [5] Shaker Alanazi ,KashifSaleem, Jalal Al-Muhtadi, Abdelouahid Derhab (2016) "Analysis of Denial of Service Impact on Data Routing in Mobile eHealth Wireless Mesh Network" in Mobile Information Systems Hindawi Publishing Corporation ,pp19.
- [6] C.-W. Lee(2013), "Security in wireless mesh networks," in Wireless Network Security Springer, Berlin, Germany, pp. 229–246
- [7] Mandrita Banerjee, Junghee Lee , Kim-Kwang Raymond Choo (2018) "A blockchain future for internet of things security: a position paper" Digital Communications and Networks ,pp 149–160.
- [8] Brijendra Kumar Joshi,Megha Soni (2016) "Security Assessment of AODV Protocol under Wormhole and DOS Attacks", 2nd International Conference on Contemporary Computing and Informatics, pp 173-177.
- [9] V. V. S. S. Balaram(2016), "A New Approach for Defending Against Vampire Attack in Wireless Sensor Networks" International Journal of Advanced Research in Computer Science and Software Engineering 6(1),pp501-505.
- [10] P.Saranya1, Abin P Varghese2, R S Balaji(2017), Detecting and preventing the wormhole attacks in wireless sensor network" International Journal of Recent Trends in Engineering & Research 03(04) pp 565-571.
- [11] S. Vij, A. Jain(2016), "Smartphone nabbing: analysis of intrusion detection and prevention systems",3rd International Conference on Computing for Sustainable Global Development pp. 2209–2214.
- [12] N. Arya, U. Singh, S. Singh (2015), "Detecting and avoiding of worm hole attack and collaborative black hole attack on MANET using trusted AODV routing algorithm", International Conference on Computer, Communication and Control (IC4), pp. 1–5.
- [13] K. Christidis, M. Devetsikiotis (2016),:Blockchains and smart contracts for the internet of things", IEEE Access 4 pp 2292–2303.
- [14] Taranpreet Kaur, Rajeev Kumar (2018)," Mitigation of Blackhole Attacks and Wormhole Attacks in Wireless Sensor Networks Using AODV Protocol" IEEE International Conference on Smart Energy Grid Engineering pp.288-292.
- [15] A. S. Toor and A. K. Jain (2016), "A survey of routing protocols in Wireless Sensor Networks: Hierarchical routing," 2016 International Conference on Recent Advances and Innovations in Engineering (ICRAIE), pp. 1-6.
- [16] S. Vidhya, T. Sasitha (2018)," Secure Data Transfer Using Multi -Layer Security Protocol with Energy Power Consumption AODV in Wireless Sensor Networks", Wireless Personal Communications, Springer.
- [17] Radi, M., Dezfouli, B., Bakar, K. A., & Lee, M. (2012). Multipath routing in wireless sensor networks: survey and research challenges. Sensors, 12, 650–685.
- [18] Xiaoqi Lia, Peng Jianga, Ting Chenb, Xiapu Luoa, Qiaoyan Wen(2017), "A Survey on the Security of Blockchain Systems" Future Generation Computer Systems.
- [19] Sachchidanand Singh, Nirmala Singh(2016), "Block-chain: Future of financial and cyber security" 2nd International Conference on Contemporary Computing and Informatics (IC3I) , pp .463-467.
- [20] Jennifer J. Xu(2016), "Are blockchains immune to all malicious attacks?", Xu Financial Innovation .
- [21] Darshana Pritam Shah; Pritam Gajkumar Shah (2018), "Revisting of elliptical curve cryptography for securing Internet of Things (IOT)", Advances in Science and Engineering Technology International Conferences (ASET).
- [22] Dania Qara Bala ; Soumyadev Maity ; Sanjay Kumar Jena (2017), "Mutual authentication for IoT smart environment using certificate- less public key cryptography", Third International Conference on Sensing, Signal Processing and Security (ICSSS).
- [23] Parmilla Subhash and S.Ramachandram (2016), "Trust based HWMP Protocol in highperformance wireess mesh networks", International Journal Network Security pp 926-937.
- [24] Mandrita Banerjee,Junghee Lee,KimKwang Raymond Choo (2018), "A blockchain future for internet of Things security:a position paper"Digital Communication and Networks pp 149-160