RESEARCHERID
THOMSON REUTERS

[Venkatesan, 5(9): September 2018]
DOI- 10.5281/zenodo.1409635

ISSN 2348 – 8034
Impact Factor- 5.070

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

NETWORK DENSITY-BASED NODE KEY EXCHANGE MANAGEMENT FOR ENHANCING SECURITY IN WIRELESS NETWORK

N.Venkatesan*[1] & Dr. M. Prabakaran[2]

[*1]Research Scholar of Bharathidasan University, Department of Computer Science, Government Arts College, Ariyalur, Tamil Nadu, India.

[2]Research Supervisor, Asst. Professor, Department of Computer Science, Government Arts College, Ariyalur, Tamil Nadu, India

ABSTRACT

The wireless network is an open medium which allows the recurrence to a few nodes. In traditional networks, the information has been transmitted to the framework, and nodes confirmation should be considered in the network. The wireless structures are one which contains specific wireless nodes other than each is an expert of sense and convey information packets. So we consider Network Density-based Node Key Exchange (NDNKE) algorithm for security upgrade in the wireless network. In this work mainly focus on the end goal to keep up forward, and in reverse protection, the group key must be changed each time when an enrollment change happens in the network. The group key must be restored occasionally with the goal that an unapproved part can't recognize the secret key. Each key being accessible in the network, the controller produces a group key which is one of a kind for the general node which is created utilizing elliptic curve cryptography and proposes a stream value based hash work which produces the key for the control stream and will be extraordinary and valuable for just the worry stream. Every time group key will be changed on source node requirement which can be estimated with the assistance of past stream keys and estimations of the elliptic curve. At the join group, the strategy distributes the elliptic curve cryptography parameters to the registered node, then group key and node demanding isolated key in the network based on the keys overall network security will be improved.

Keywords*: Key, density, cryptographic, elliptic curve, Wireless network.*

I. INTRODUCTION

The wireless network offers a lot of services and functionalities to the enormous amount of users in a real world by conceiving the variety of methods.These methodologies are slacking by giving proficient access control arrangements and time many-sided quality issues with the greater part of its supporters. To conquer these issues, the plan called key administration with period has been given here. This thusly enhances secure data exchange utilizing elliptic bend cryptography.

In this plan, for each communicate benefit, the arrangement of elliptic bend properties are created and doled out with starting qualities at each session. Data exchange conventions guarantee secure correspondence by encrypting data in two normal ways in particular square and network thickness. The first encrypts rise to measured data as a square at one time, and the span of the first content is littler than the squares at that point cushioning bits are included. While the second one encrypts the data it is possible that one piece or byte of unique form at once and consequently a few distinctive keys are expected to get the vital current network. Security astute the last number is more inflexible than the previous in light of the fact.

The fundamental services on conspire utilizes a changed number of keys for an alternate arrangement of clients per session. What's more, again the session time fluctuates in view of the substance of being transmitted. The separate or group of people who preserve the network and its security must have admission to every area of the scheme.

Therefore, the security policy organization function must remain allocated to people who stay enormously trustworthy and should have the necessary technical capability. As noted earlier, the popularity of network security openings come from within, so this being or group must not continue a possible threat. Once assigned, network managers take benefit of sophisticated software tools that can help define, dispense, enforce and audit safety policies of complete browser-based interfaces. Encryption innovation affirms that messages can't proceed with captured or perused by anybody other than the official beneficiary.

Encryption is typically composed to ensure data that is passed on finished an open network and uses progressed correct calculations to "scramble" messages and their extras. A few sorts of encryption calculations exist, yet some keep on more secure than others. The communicate will assume a significant part in the up and coming age of networks the same number of administrations, for example, pay-per-see media communicates and the conveyance of network control messages will depend upon bunch correspondence.

One security benefit that has been hard to accommodate transmission is validation. Maintaining the high security are tedious in situations like setting up access control policies, providing trustworthiness in groups and whenever dynamic changes occur in such networks. Although the node to node communication offers the excellent solution for broadcast security, still it is incompetent, and it eliminates routing for broadcasting in wireless networks. Hence, efficient routing protocols have been used, and that reduces the network overhead at the minimal level.

II. RELATED WORKS

Security confirmation events such as essential collection procedures, balanced encryption-decryption facilities review events, and then transmission confirmation events remain likened and inspected for all safe transmission requests [1]. This amount rations the corporeal of steering swapped amongst the nodes. Approving secure declaration among wireless applied beforehand the Internet like a threatened declaration groundwork aimed at wireless sensor network and significant uninterruptedly using encryption then necessary symmetric encryption [2-3].

This scheme secures group communications by performing crucial public encoding using ECC with secret key exchange algorithm which is applied at various levels of network construction [4]. The encryption method with hyperelliptic curve cryptography dealt with security requirements such as authenticity and confidentiality in a platform and resource-constrained devices [5]. A technique called encryption which performs both digital signature and encryption simultaneously is designed to achieve low communication cost and other resource requirements like storage and lifetime of mobile environments.

Earlier authentication schemes and initiation protocols did not resist spoofing, password guessing attacks, etc. [6-7]. So, this method proposed a new and enhanced authentication technic by using a hard elliptic curve discrete logarithm problem on session initiation protocol to secure and safeguard the information from various attacks. Al the data should be collected into another node where each node serves as a sink for others. But generally, they all suffer from limited bandwidth, limited lifetime and frequent denial of communication [8-9].

All these drawbacks were addressed in this system through different types of routing protocols such as location-based, data-centric routing, hierarchical routing, and energy aware and geographical routing [10-11]. In various security threats and challenges faced by unattended sensor nodes in wireless infrastructure. The focus is mainly given to the review of all the significant security measures such as verifiability, availability, integrity, and confidentiality [12-13].

Crucial efficient establishment and distribution techniques must be designed to surmount several possible attacks eavesdropping attack, tampering attack, denial of service attack, routing attack, physical attack, etc. Several security mechanisms have been explored to withstand these attacks [14-15]. It taxes the expenses of hierarchical building and obtains a two-level significant cluster alongside validation arrangement, the valuable possessions but likewise protects scalability.

Group head should spontaneously give responses whenever multiple requests are coming from many subscribers by controlling all other subordinate nodes [16-17]. It suggests a significant trust in private authentication and key management based on asymmetric methods and is not capable for the node to node security in wisdom web of things in wireless sensor networks. Hence, the scheme uses a crucial public way for them to minimize the overhead and power consumption in sensor nodes [18-19]. It is nervous that the focus levers only control traffic. The files packs continue routed using existing broadcast steering protocols. Encryption can remain done using a key common for all members [20].

III. MATERIALS AND METHODS

The Network Key Exchange is created by the node density based key control scheme are mapped with elliptic curve qualities with the group key are dispersed to the registered nodes, when they are participating in the group at current density. Each time window, the different arrangement of keys are produced similarly and given to every one of the nodes. At the receiver side, the private keys are utilized to decrypt the elliptic curve parameters to get the first substance. The proposed strategy is divided into three different parts for better security; they are Density Analysis for Group of Nodes, Key generation Based Encryption and Decryption and Key Modification for Data transmission.

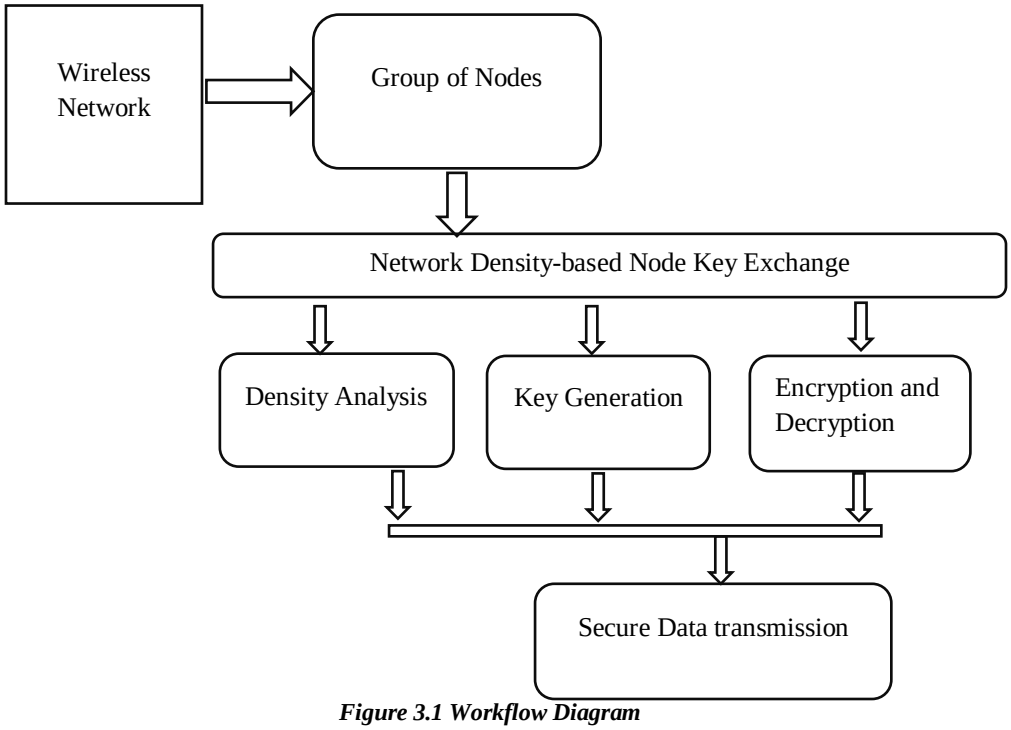

Figure 3.1 Workflow Diagram

The above figure 3.1 shows the essential component of cryptographic-based security enhancement for the results help to understand the limitations of the analytical results based on the collaborative, secure data transmission into the study and analysis of network that utilizes dynamic data distribution.

3.1 Density Analysis for Group of Nodes:

In this work first stage is density examination for the group of nodes, it's fundamentally to group all nodes in the information of its necessity. At the point when the node wishes to wind up an individual from any group, first, they need to send joining request to the group head and sends the current sessional curve parameters, the density estimate alongside the chose key. Based on these qualities the processed attributes are transmitted to the base station from that point, the beneficiary registers the encryption and decryption key for the next stage.

Algorithm

ISSN 2348 – 8034
Impact Factor- 5.070

input: Node in number Nn
output: Network Density Nd.
Start
Produce group join request Jr = {node id}.
Obtain Answer Jr.
Accept ECC Limits for each node
Remove Maximum data loss node Mdl = Jranswer (Nn)
Build the network density Size Nds = Mdl(Jr).
Stop.

Crypto investigation of secured appropriation framework moves the grouping time access and security to the massive server fields, where the connection of the nodes requires the information and security controls may not be entirely uncomplicated for security concerns. In this crucial multi-group express that common event point on wireless network security, which has been continuously an essential part of the learning of security benefit.

3.2 Key generation Based Encryption and Decryption:

In every node, the group head creates and introduces the elliptic curve properties with various qualities chose on curve point, and these are distributed to the selected group who require the arrangement of keys. The location which is selected on the curve is mapped with the keys, and these are later utilized for doing encryption and decryption. And furthermore, these arrangement of keys are substantial just for the present time frame. Along these lines, for each new method of keys created and appropriated and this maintains a strategic distance from data loss.

Algorithm:
Input: network density Size Nds
Output: Key generation Kg.
Start
Prepare network node Nn.
Recognize set of all nodes.
Nn = $\int \sum Jrrequest \in Network$
For each node Ni from Nn
Preparenode id.
Adjust ECC parameters.
Calculate network group size Gs.
Gs = $\int Max(Jrrequest)$
Compute Key of the all nodes Kn = $\sqrt{(Nds1 - Mdl)}$
Kg =Kn+Jr+Nn.
End
Stop

Each node that is rights has a place with the group determine the key utilizing some essential requirement. If an amount of transmitting message gets the loss that is not checked, at that point node are as yet capable of displaying symptoms of improvement. The group key for that session by utilizing the update they built up at the opening of past get together time end and the announcement they will reach or sharing the security key, without asking for the extra details from the group head also conventional key won't prepared.

ISSN 2348 – 8034
Impact Factor- 5.070

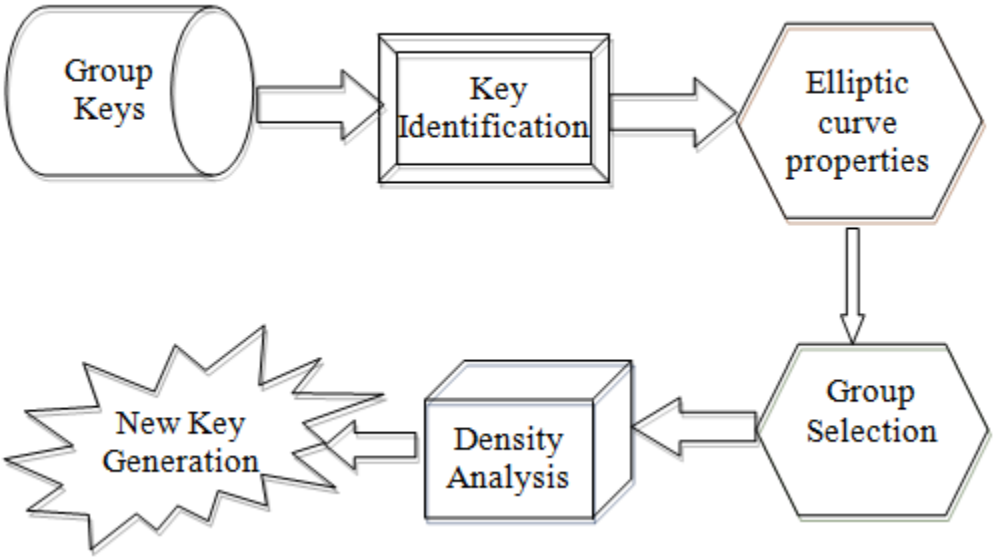

Figure 3.2 Stages of group key identification

Figure 3.2 demonstrates the confidentiality to stay at both the sender and the recipient side while encoding and decoding the data. Classification exists in two different ways like forward and reverse. The forward prediction utilizes here and now key trade and confirmshistoricalmeetingsin contradiction ofpredictablestandards of underground keys since the communications sent to receivers are encoded with the same arrangement of open keys over and over. This influences the opponent to choose the design content to movement protection in concentration the terminationarea to decode the data in the network.

3.3 Key Modification for Data transmission:

In this stage looked over elliptic curve is included with the created set of keys and this needs some change done in a key. This technique requires two nodes measure estimations of source and destination. By utilizing this arrangement of qualities the useful parameter to exchange the information and registered a method of the symmetric key is used for achieving encryption. Also, on the beneficiary side, the fact of the matter is first processed and using same capacity it determines a similar set key which is used to decrypt the first message.

Algorithm:

Input: Key generation Kg

Start

If Kg==1

Add Alteration among $Nds\ and\ Mdl.$

Collection group Cg = $\sqrt{(Kg(Jr) - Nds(Kg))}$

Else

To choose intermediate node In = $Network\ density + \sqrt{Kn - Mdl}$

End

Recognize the node Rn = In (data transfer).Value

Stop.

At this period, the technique gets the information about elliptic curve parameter, highest density, and current network measure. The scope of qualities between the two node sizes, the new arrangement of key attributes are registered by utilizing node density, and these are being used to decide the encryption key or decryption key. The

present network represents the limit of every node, as per this, the keys are registered. Thus, for decryption, the key will be developed by finding the contrast between the qualities indicated in the purposes of the security.

IV. RESULTS AND DISCUSSION

Proposed approaches is run simulated using network simulator, then the all code are created in to TCl script. Based on the simulated result the given output simulated result is taken. Our proposed (Network Density-based Node Key Exchange (NDNKE)) framework is contrasted and three existing frameworks; they have Distributed Secret pivotal sharing-based administration (DSSKM).

4.1 Packet delivery ratio Impact:

It's used toward survey idea through the framework. It represents extent amongall packetsin thenetwork. In source to destination how many packets will be send in particular time it's called delivery ratio.

PDR = Packets received/Produced parcels * 100

Table 4.1 similar examination

Figure 4.1 maintain the result of planed work with simulated output. NDNKE has a normal increment in PDR of 9% through the present DSSKM.

Node in No	DSSKM in %	NDNKE in %
20	13	19
40	26	46
60	48	55
80	65	78
100	82	91

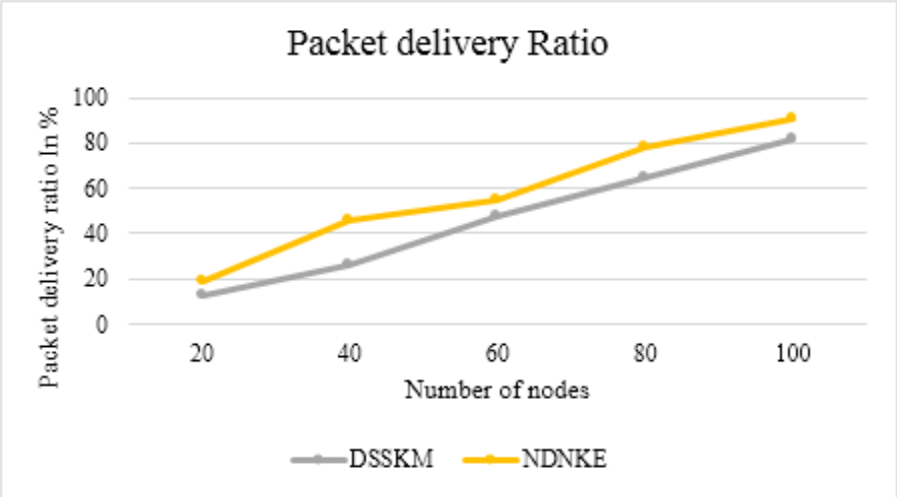

Figure 4.1 Comparative Analysis

ISSN 2348 – 8034
Impact Factor- 5.070

4.2 Examination of End- End Delay

End to end delay is nothing but between the times to taken from one packet to another packets in network. That time to take all kind of parameter in data transmission.

Table 4.2 exhibitions the conclusion to termination defer examination of the planned framework with the current frameworks.

Table 4.2 End to End Delay

The rate of Sending Packets/sec	DSSKM	NDNKE
10	0.866	0.755
20	5.648	4.654
30	8.254	6.214
40	9.754	8.648
50	9.866	8.964

Figure 4.2 exhibits the E2E examination of the prearranged schemes with the present structures.

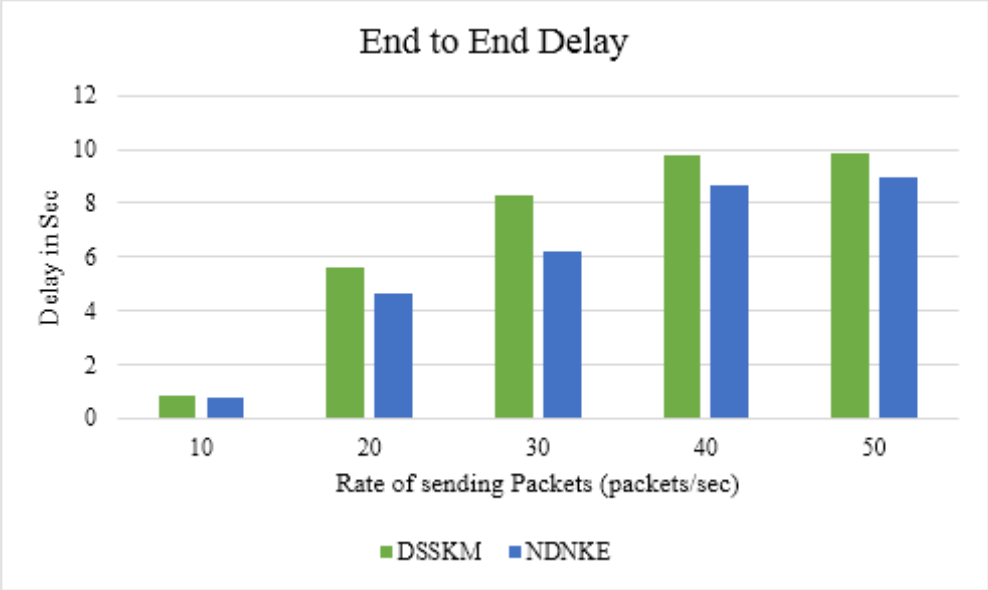

Figure 4.2 End to End Delay Ratio

Since Figure 4.2 obviously understoodplanned NDNKE consumes lessened this one conclusion of the packet transmission.

4.3 Throughput Ratio

Sometime called over all network performance is called throughput ratio, its consider all the QoS parameter to conclude the result in network.

Table 4.4 demonstrates the throughput proportion examination of the suggested framework innetwork.

Table 4.4 Analysis Table

No.of. nodes	DSSKM in %	NDNKE in %
20	12	19
40	26	35
60	45	53
80	66	71
100	89	92

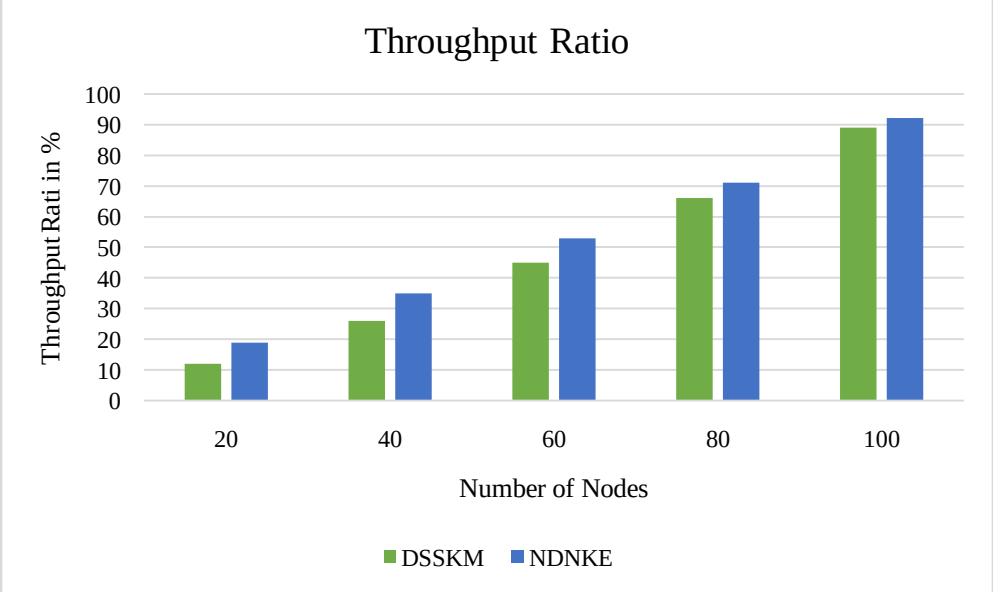

Figure 4.3 Throughput ratio analysis

Figure 4.3 demonstrates the qualifying examination of the throughput proportion of the arranged structure with the staying, in light of the qualities is given below.

V. CONCLUSION

The arrangement of node exists on the elliptic curve at various focuses are considered as the keys, and the calculation of this is finished by utilizing the network density. The discussions are picked arbitrarily from the elliptic curve, and the esteem introduces at each point discourses to the present network estimate and the greatest at whatever point the new key of information is chosen. The new node gets the scope of qualities between these two qualities. The arrangement of recently distinguished conditions is utilized for encryption and decryption. For every session, a similar method of tasks is performed over and over with new a few distinctive techniques of keys which are chosen on the elliptic curve. Along these lines, this plan limits the time multifaceted nature and produces successful outcomes in the altering accuracy, from the analysis, it is clearly shown that the proposed NDNKE has improved its throughput ratio to 3% which is compared with the existing system.

REFERENCES

1. *Amit Kumar Singh, 'Identity-Based Key Distribution for Wireless Sensor Networks using Cryptographic Techniques', International Journal on Emerging Technologies, ISSN 0975-8364, vol. 6(1), pp. 69-72, 2015.*
2. *Prasant Singh Yadav, "Implementation of RSA Algorithm Using Elliptic Curve Algorithm for Security and Performance Enhancement," International Journal of Scientific & Technology Research Volume 1, Issue 4, May 2012.*
3. *Anwar Ghani & Husnain Naqvi, 'An efficient encryption scheme with forwarding secrecy and public verifiability based on hyperelliptic curve cryptography,' Multimedia Tools and Applications, vol. 74, no. 5, pp. 1711-1723, 2015.*
4. *Bertier, M, Mostefaoui, A & Trédan, G, 'Low-cost secret-sharing in sensor networks,' in Proceedings of the IEEE 12th International Symposium on High Assurance Systems Manufacturing (HASE '10), pp. 1-9, 2014.*
5. *Shanthi S and NagenthraBabu, "Secure Data Retrieval in Wireless Networks Using Advanced Encryption System," International Journal of Engineering Development and Research, ISSN 2321-9939, 2015.*
6. *Feinstein L, Schnackenberg D, Balupari R & Kindred D, 'Statistical Approaches to DDoS Attack Detection and Response,' Proceedings of DARPA Information survivability conference and exposition, Washington DC, pp. 303-314, 2003.*
7. *Gilad V & Herzberg A, 'LOT: A against IP Spoofing and flooding Attacks,' ACM Transaction on Information Systems, vol. 15, no. 2, 2012.*
8. *Deepak Dembla, 'Modeling and Analysis of an Intelligent AODV Routing Protocol based on Route Request Retransmission Strategy in MANETs', www. JSOnline. Org/archives/volume30 / number11/3684-5190, 2012.*
9. *Tahir M.Y and Javed, "Rabbit-MAC: Lightweight Authenticated Encryption in Wireless Sensor Networks," International Conference on Information and Automation (ICIA'2008), pp. 573-577, June 2008.*
10. *Tejinderdeep Singh, 'Detection and Correction of Sinkhole Attack with Novel Method in WSN Using NS2 Tool', IJACSA, vol. 4, no. 2, 2013.*
11. *Shushan Zhao, 'A key management and secure routing integrated framework for Mobile Ad-hoc Networks,' Elsevier, Ad Hoc Networks vol. 11, no. 3, pp. 1046-1061, 2018*
12. *Raja Rajeswari S and Seenivasagam V, "Comparative Study on Various Authentication Protocols in Wireless Sensor Networks," The Scientific World Journal, 2016.*
13. *Newsome J and Shi E, "The Sybil attack in sensor network Analysis and defenses," International Symposium on information processing in sensor networks (pp. 259–268). Berkeley, CA: ACM. 2004.*
14. *Padmavathi D and Shanmugapriya, "A Survey of Attacks Security Mechanisms and Challenges in Wireless Sensor Networks," (IJCSIS'09) International Journal of Computer Science and Information Security, vol. 4, no. 1-2, 2009.*

15. *Sanjay Sharma & Pushpinder Singh Patheja, 'Improving AODV routing protocol with Priority and Power Efficiency in Mobile Ad hoc WiMAX Network,' International Journal of Computer Technology and Electronics Engineering (IJCTEE), vol. 2, no. 1, pp. 87-93, 2012.*
16. *Walid Abdallah and NoureddineBoudriga, "An Efficient and Scalable Key Management Mechanism for Wireless Sensor Networks," ICACT Transactions on Advanced Communications Technology (TACT), vol. 3, no. 4, 2014.*
17. *Sari A and Onursal O, "Role of Information Security in E-Business Operations," International Journal of Information Technology and Business Management, 3, 90-93, 2012.*
18. *Qi Dong and Donggang Liu, "Mitigating jamming attacks in wireless broadcast systems," Wireless Networks, vol. 19, no. 8, pp. 1867-1880, 2013.*
19. *Raghavendran, CHV, 'Intelligent Routing Techniques for Mobile Ad hoc Networks using Swarm Intelligence,' International Journal of Intelligent Systems and Applications (IJISA), vol.5, no. 1, pp. 81-89, 2012.*
20. *Makhmali A and H.M Jani, "Comparative Study on Encryption Algorithms and Proposing a Data Management Structure," International Journal of Scientific & Technology Research Vol. 2, No. 6, 2013.*