Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 3, July 2021:1271- 1283

Research Article

An Advanced and Shared Cryptographic Technique for Security enrichment in Ad hoc Networks and Mobile Application

P Kalaivani[1], Nithya J[2], Ramya J[3]

Abstract

A communication based systems are distinctive information systems, which might be undermined through the illegal users who contain prohibited access in the direction of the systems. The proposed method uses the role- oriented access organized framework with the collective cryptographic primitives. A cryptographic based puzzle component along with a key - oriented module, is used protect the traffic pattern that are transferred during the MANET. The source node sends the packet data towards the wireless based channel along with the combined said cryptographic techniques. A node that wants to get the interchange pattern must answer these two kinds of primitives. At first it resolve the puzzles of cryptographic and next it answer the key-oriented scheme (that is symmetric based encryption) after that it can be capable of accessing the traffic of data pattern packet that send above the MANET. This kind of scheme is well-matched with the packet broadcast; the storage and it acquire a low power utilization. In this experiments, it has been demonstrated with the aim of combining the cryptographic oriented method for the key based and the Puzzle related methods which provides better way of security, because it employ the dual - guarded way of the security, consequently that it give an efficient and the secured way to system for MANET**.**

Keywords— *TrafficAnalysis, MANET, Merklle's Puzzles,Key-based, Cryptographicpuzzles, Encryption based scheme*

[1]Assistant Professor, Department of Information Technology, Bannari Amman Institute of Technology, Erode, Tamil Nadu. kalaivani.pachiappan@gmail.com
[2]Professor, Department of Information Technology, K.S.Rangasamy College of Technology, Tiruchengode, jknithya@gmail.com
[3]Assistant professor, Department of Electronics and Communication Engineering, Hindusthan College of Engineering and Technology, Coimbatore, Tamil Nadu. ramyaresearch12@gmail.com

Introduction

A Mobile Ad Hoc Network (MANETs) be a compilation of quantity of nodes or the devices or the terminals with the wireless based communications and the networking capability that the converse with the each other with no help from any other centralized way of manager, as well the wireless kind of nodes which could be dynamically outline a network toward the conversation of information with no usage of any of the existing permanent networking structure.

A MANETs can exist the use of the global way of scaling for habitation study and the monitoring of environmental factors, that might over a conflict field intended for the military observation and the investigation, used in the emergent environment that explores and release, in the factories designed for the condition oriented maintenance, inside the buildings for transportation, inside the homes to understand the smart homes, otherwise yet in the bodies for monitoring of patient. An assailant can duplicate a picky tag after answering the cryptographic kind of puzzle sent by it. But, the success ratio of this attack is zero when that was the amount of tags been increased since the surplus time inspired in solving every associated puzzles.

This may seem towards the readers of the methods that the honest transceivers will be suffered with the similar problem. Though, the truthful readers (in the nearest environments) have been accessed to the way of accessing the back-end kind of database that can be provided by them with the part of the key that belong to those tags that are registered towards the system. An efficient and widely secured, but bit slower, scheme of discovering the key could use the client puzzles which will be of Merkle based puzzle. In support of each of the node could be a problem for the client based puzzles (each one for the m keys) toward each of the neighboring node.

A quantity of node which responds through the accurate answer to puzzle's client is been identified because significantly the connected key.

The multi-path based routing is the main procedure for the data reliability that forwards in the prone to the failure in wireless sensor kind of networks (WSNs), that leads to the consume of huge energy. Here a new mechanism of routing which combines the multi-path based routing with the network based coding (NCR). This type of understanding decreases the required number of path and the total times of the WSNs transmission. In the NCR, encoded packets at the source nodes be transmitted on top of the multi-path in the direction of the descend.

This method uses the algorithm with controlled hello packets, to find out the necessary paths from source to sink node and nodes avoid the use of any explicit response message and the number of control messages which exchange between nodes for route discovering, has been reduced, which it leads to consume lower energy. Simulation results show that NCR enhances the consistency, reduces the number of transmission paths and improves load balancing in WSNs.

One of the main challenges faced by a multipath routing scheme is to decide how to split the rates among the multiple paths. This rate control algorithm must adapt quickly to varying link qualities, congestion signals from different paths, and packet losses. Rate control is similarly needed to prevent forwarders from producing more information than they received. This could create an information overflow with many linearly reliant packets flowing over the mesh across altered paths. Rate control should also allocate network resources properly among challenging flows. Multi-path routing is an important technique for dependable data forwarding in prone to failure wireless sensor networks (WSNs), which it leads to consume more energy. In this research, the system proposes a new routing mechanism that syndicates multi-path routing with network coding (NCR) [3]. This combination decreases the number of required path and the total times of transmission in

WSNs. In the proposed algorithm the number of control messages with the arguments between the nodes for determination of route that has been minimized. The results of the simulation represents the value of NCR been the energy-efficient technique which enhances the parameters of the similar kind of the multi-path based routing protocols.

The proposed system considers a Multipath based Network Coding (MNC), a control of rate and the routing protocol which radically improves the throughput of the lossy based wireless networks. With the OMNC which employs a lot of paths to be pushed with packet coded towards destination, in addition to the uses of the transmission of MAC that delivers packets among the adjacent nodes. The broadcasting and coding is allotted to the transmitters through the dispersed algorithmic optimization which make use of the development of the path assortment while keep away from congestion. By means of extensive experimentation by the emulation way of test bed, it finds that the MNC attains the important of throughput enhancement over the conventional greatest routing path protocols and the prevision based multipath routing kind of protocols with the network coding [4].

With the MNC, the cause node continuously engenders the packet streams as of a collection of data that lumps with a random kind of linear code (RLC). A Coded based packet streams through the multiple kinds of paths to the destination end. Intermediate way of forwarders can revive the streams of packet by way of re-encoding the existing packets and the broadcasting packet code to the downstream nodes. With the adequate packet number of build up at destination end, actually group of the data blocks that can be improved. Then, an ACK based uncoded is been sent back in the direction of source (if possible using the traditional best path based routing), that allows it on the way to start the operating with a new collection of the data blocks.

Literature Review

The STARS: The Statistical kind of Traffic Pattern based Discovery System for the MANETs that work inactively to execute traffic analysis with the statistical appearances of the captured raw traffic. With these methods, it recognizes the definite source node and the destination based nodes, and relates source nodes by means of their equivalent destinations. The approach of STARs is a statistical way of traffic based analysis which provides the method that takes a most important distinctiveness of the MANETs broadcasting objects, the mobile and ad hoc property. The STARs is been an system of attacking which classify every nodes of source and destination which determines the association between them. With the previous mechanism, the traffic model of analysis been extensively exploited with static wired based networks [5]. Consider an example, the method to trail a message for capturing them with one by one every one way of possible paths with a message that could be traversed, namely brute force based method . Excluding passive nature of numerical analysis of traffic attacks is been very accepted. At the present attackers only require to gather information and execute statistical analysis of traffic mutely without adjusting the characteristics of the network.

The demerits of the existing methods are:

- Network coding benefit is esteemed only but there be traffic in equal directions of the path shared.
- Consumption of energy is huge when connected with the proposed technique.
- The major problem of presented method is the way of make simpler statement for PHY and the MAC.

Proposed System

The proposed System aims to construct a traffic management in a distributed method that would be the source node that with each flow could divide its traffic, (the packets per unit time), amongst the multiple dissimilar paths. Consequently to minimize the cost of the system, the total transmissions number per time essential to maintain a known traffic

demands. This system formulates the purpose of cost minimizing, subject to requirements of the traffic of each flow, as an optimization in complex manner.

The method proposes to incorporate the mobile agent methods with the multi-agent method to improve the capability of management of traffic systems which deals with ambiguity in a lively environment. Still the agent technique been contributed to improvement of management of traffic, the implementation, the design, and the application of the agent-oriented techniques in this spot are still young which ts to be needed for further studies. With this approach, the method system reduces three problems: the capability to the interoperability, hold the extensibility and the uncertainty of agent-oriented distributed management of traffic systems.

Different as of motionless agents, the mobile based agents are able to transfer from single network node to the other nodes that are to be alive accomplish with any of the network nodes. Mobile based agents could be complete dynamically on the runtime and transmitting to the destination based systems to execute the tasks with the most efficient code and the algorithms [7]. The mobility enhances a great chance to deal with the challenges in the management systems and the traffic control, such as fast incident based diagnosis, organizing a new way of algorithms or operations that is been dynamic, dynamic method configuration taking unanticipated actions with dropping the data transmission in a network.

Mostly all the existing agent-oriented traffic management based applications are been based on the multi-agent based systems. These methods consist of the different functional based stationary agents who are been supportive and intelligent. The synchronization between the agents is been attained during some certain kind of the protocols. An agent based method constructions comprise with simply interacting based agents, a centralized based architecture, and the decentralized based architecture.

A public-key based cryptosystem be useful for the statement so as to it strengthen is possibly to discover a method where it is been computationally impracticable to decide the rule of decryption specified to its rule of encryption. Thus, the rule of encryption be a public way of key that could be available in the directory while the rule of decryption be key of private which is said to exclusively through the recipient. The encryption is an act of text encoding consequently that the others not be privy to decryption technique (the "key") that is not been appreciate as the text satisfied. Encryptions have long with respects to area of diplomats and spies, followed by not long it have been moved with the open eye with unrest protection of the electronic based transmissions with numerical data stored. The standard way of encryption scheme typically have two essential errors (1) The protected channel have got to be familiar at some position so as to the dispatcher may swap the key for decoding by means of the recipient; plus (2) There be no declaration that whom sent a particular message. The public key based encryption has a fast grown in recognition because it proposes a much protected based encryption scheme which addresses those disquiet.

The RSA be a public-key based cryptosystem which supports both digital based signatures and encryption. Comparable to every public key based cryptography methods, the RSA based cryptosystem that encrypts and then decrypts the message with the help of a keys pair which recognized as the public based key and the private based key [8]. This type of security is a kind of complexity of factoring huge number of integers. Currently, the most accomplishment of RSA based algorithm utilizes the employ of the 512-bit of numbers. The furious methods involve the capability to the factor of the creation of both the 512-bit based prime numbers. The factoring aspects of numbering this dimension are well outside the ability of the most excellent present factoring based algorithms.

The reward and merits are:

- The proposed methods considerably decrease the cost.
- It implements the constraints as glowing.

- The proposed dual -level controller congregate quick to the finest solutions.

The Key and Cryptographic Based Puzzle Design

A. The Network Configuration

The networks are produced with the specified variety of sensors. The nodes be grouped robotically depends leading their radio based waves. An agent is shaped for the collection of registration. In the wireless based networks, even while the broadcasting allows simultaneous communication to nearest nodes, it equally acts as interfering at these kinds of nodes which are take noted to some node rather than the mode of broadcasting. This kind of interfering in wireless based networks, called the Co-Channel kind of Interfering, it is handled with a greater MAC based protocols (for the example named CSMA) so as to list the transmission phase of relations in network which that interfering is diminished. This method assumes that a ideal schedule of the wireless relations is known and, consequently, there is refusal interfering in the recipient. However, this inflicts self-possession on the utmost number of communication per unit time resting on nodes.

B. The Cryptographic Puzzle based Scheme

This methods uses a Merklle's based Puzzles to cover the interchange pattern because the pattern of traffic environs the destination, source, end-to-ending communication association details. While the node imprisons the traffic, then it wants to answer the puzzle therefore only authorized users who recognize the puzzles solving based scheme. The cryptographic kind of puzzles are famous method, but it is the primary time-to most excellent of the acquaintance- so as to use is been proposed within the circumstance of the RFID based schemes. An encryption kind of function is been engaged intended for the production of cryptographic based puzzle. Consider the example; presume Alice and Bob desire to relocate. The Bob who can able to throw a message in the direction of the Alice since tracked: initially it generates a huge amount of the puzzles, correspondingly to a restrained quantity of complexity — it have got to be likely for the Alice to answer the puzzle by means of a reasonable quantity of calculative purpose. Puzzles be in the shape of the encrypted kind of message with an key that is unknown; the key be obliged to exist little adequate to authorize a brute force kind of attack. The Bob that sent the question to the Alice, with a selection of one arbitrarily, and it is solved.

An Encrypted based solution hold an identifier, that an assembly type of key, as a result of the Alice can converse reverse to Bob that the puzzle been solved. Together the events at the present of having a common type of key; The Alice, because she had solved a puzzle, and the Bob, because he had sent the puzzle. A kind of any eavesdropper (Eve, declare) have a tough task — she do not recognize which of the puzzle been solved by the Alice. Her most excellent approach is to answer all kind of puzzles, except subsequently here is consequently a lot of, this be a more calculative expensive intended for the Eve than for Alice. The cryptographic based puzzles are the puzzles been used to conceal a top secret which be able to merely be exposed after some calculative attempt be made. The Ralph Merkle considers the primary Puzzle scheme to make sure that the two kinds of parties can converse a securely in excess of the insecure way of channel.

The calculative kind of puzzle be reasonable tough problem, the respond of that can exist calculated contained by the rational time and been verified proficiently. This kind of problem is frequently known to the requester of the service been solved before services are requested is being provided. Two kinds of parties' determination will agree on the shared top secret by swapping the messages. The Merkle's based puzzle has a mass of the puzzles in the encrypted form of message through the unknown based key. The puzzles use the one-way based encryption purpose while the key have to been short sufficient to permit a brute force

based attack. The cryptographic based puzzles have different applications in security field. This are wide usually used in get rid of the denial of the services that attacks with many researchers have been also projected the cryptographic based puzzles usage in fighting the association reduction attacks.

C. The Key-based encryption method

Behind the solving the puzzle be able to confine the announcement pattern be able to discover excluding it does not be hold the original kind of format because a key oriented encryption method is been used to secrete the pattern of the traffic packet. To achieve the original format frame user have to recognize the method of solving the particular kind of key methods used. The standards of cryptographic based hardware and software is been used to do encryption. Different cryptographic based algorithms that are being utilized to secure the data including video and images, excluding all of these having few advantages and disadvantages. The novel symmetric based key cryptographic technique is intended for the encryption and the decryption of every file that covers the numbers, symbols and the characters. Numerous cryptographic based algorithms are being focused on data text. The cryptographic based algorithms that are used for the secured way of text messaging with the data that are not good video, audio and images based data applications since large sizes of data and the real time restriction.

The kind of digital signatures that are equivalent to the conventional signatures of handwritten in the numerous respects, other than the properly implemented the digital based signatures that are more demanding to falsify than the type of handwritten. This kind of methods, which are used now, that is cryptographically been based, and the must been implemented correctly to be prepared. The digital based signatures could be also deliver the non-repudiation, significance so as to signer that are not effectively claimed that are not in signing the message, as also tempting to their key of private that remains to be secret; additional, some of the non- repudiation methods present a time stamp intended for the digital based signature, consequently the level in which the private based key is observable, the validation of signature is done. The digitally signed kind of messages might be anything corresponds to be a bit a way of string: the examples comprise the contracts, a message or electronic mail, that is sent through some of the other kind of cryptographic based protocol.

D. The Established Routing path

After the completion of solving the puzzle and also the solving key scheme completing the node that could access the pattern of communication as well as establishment of routing that depends in the lead of information of destination restricted in packet. At this moment, a table of routing been recognized in every node that contains the routing information with every other in the network node and those information's are updated infrequently. Behind the common susceptibility of the wireless based connection, and manet based network have its own detailed security issues owing to malicious neighbor dispatch kind of packets. A characteristic of the distributed kind of operation requires variety schemes of key based management with authentication techniques [9]. Additional, the wireless link uniqueness also be introduced the reliability based problems, since the limited kind of wireless range of transmission, the nature of transmission of wireless based medium, with the mobility- related based packet losses and data kind of transmission errors[10].

E. Analysis

In this phase, a comparative based analysis is been completed for the competence of the proposed methods such as the puzzles based solving, different key based management methods. The proposed methods deals with the different levels of security are also examined.

The performance based metrics like accuracy, throughput, Energy-efficiency, delay, are been examined. The performances of topological network and the constraints of routing which are to be measured throughout the network based simulation [2]. Different constraints of security are been examined and the attacker kind of behavior in node is examined in the case of the throughput. To conclude the comparative way of analysis is absolute with the accessible and the proposed method. Based on the results of simulation examined which are finished and the results be obtained so as to the proposed method provides a tough security mechanism when match up to by means of the existing one.

The concepts of the digital based signature algorithm is

- $p = 2^L$ be the prime based number, where L value= 512 to 1024 bits and be a multiple of 64
- q - 160 bit prime factor of p-1
- $g = h^{(p-1)/q}$ in this h is a number that is less than p-1 with $h^{(p-1)/q}(\text{mod } p) > 1$
- x - number less than q
- $y = g^x(\text{mod } p)$
- generate a random k, k<q
- that compute
    - $r = (g^k(\text{mod } p))(\text{mod } q)$
    - $s = k^{-1}.SHA(M) + x.r \text{ (mod } q)$
    - the signature is (r,s) **to verify** a signature:
- $w = s^{-1}(\text{mod } q)$
- u1= (SHA(M).w)(mod q)
- u2= r.w(mod q)
- v = (gu1.yu2(mod p))(mod q)
- if v=r then the signature is verified

The analysis about Puzzle cryptography Algorithm: 1)The sender

S - Sending a packet m to receiver

R - By selecting the random key k{0,1} and generate the puzzles as follows.
P=puzzle(k,tp)

Puzzle() function has 2

to sign a Message M

parameters. k –Random key and tp-timestamp

2) Now sender broadcast P to network along with cipher text
CC= Ek (π,(m))

3) At the Receiver ,it will received C' and P' 4)Receiver First solve the puzzle
K'= solve(P)

5) Receiver then convert cipher text into Plain text

The DoS mitigation method is been proposed in (Xiaox which is used in digital signatures to been verified by the reasonable packets, with the drop based packets that have not overtake the verification process. The network determined is been formulated [1] that which nodes are laterally a path of network, which are inspired to proceed together to the screen out awful packets arrange to optimize their individual benefits.

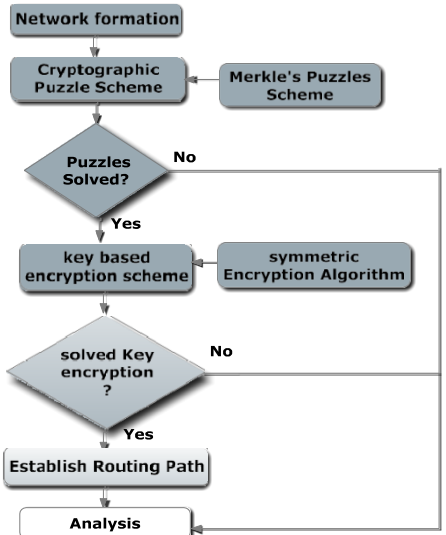

Figure.1 Architecture of An Efficient Combined Cryptographic Approaches for Security Enhancements In Adhoc Networks

In this method it follows a similar description used in the game theory [6], where set of players 1,2,3, a set of potential strategies1 2, ,...,nS S S for each player and the payoff for every consortium methods. Based on Figure 1 assumption that 1 node that from at the present on determination be referred be 1P, needs to converse with the 2 node (2P). The 1P transmits to 2P be its ID, a message hello, Man d be the timestamp be 1T.After 2 Perceives those three kind of parameters, it produces a random based prime number p, the generator of *p type and x a random integer. Previous sets kind of complexity level d of puzzle which 1P have to solve it. Subsequently, the 2 P compute the value y related to the statement (1) as follows: The xy g mod p (1) with the responds to the 1P by sending 2, ,g y p T d.While,1P get,g y and p resolve equation (1) through the baby-step and the giant-step algorithm which is determined (Stinson, D. R. 2002). Subsequently, the 1P calculates the division integer of x and d in the puzzle (i.e./x d) that equals to the number n which is required to generate the puzzle approach. After the finding, 1 P will be accountable for producing and to solve the puzzle. It suggests that 1P will be first needed to examine all the strategies that the Sand second to discover the most favorable approach opt S.

Performance Evaluation

A) A number of attackers vs. The Routing Overhead

The graph, shows the proposed method is well-organized with the Existing scheme. In the Number of attackers Vs. the Routing overhead, the graph explains when the attackers number is increased when compared to that of the routing overhead also be increased. Therefore, this paper finishes with the results that, the proposed method is very highly effective than the several other existing methods.

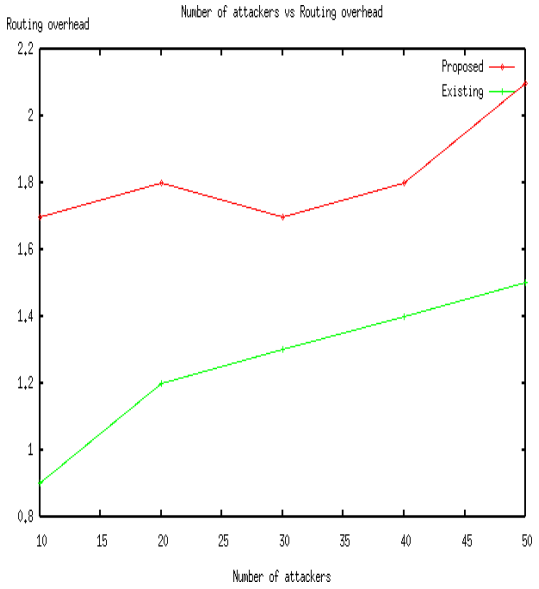

Figure.2 Attackers vs routing overhead

B) The Number of attackers vs. the Throughput

From the mentioned graph, shows the proposed scheme is competent than the Existing method. In comparing Number of attackers vs. the Throughput, the graph explain when the attacker number increases then the throughput too increases. Therefore, this paper concludes, which the proposed method is extremely capable one than the remaining methods.

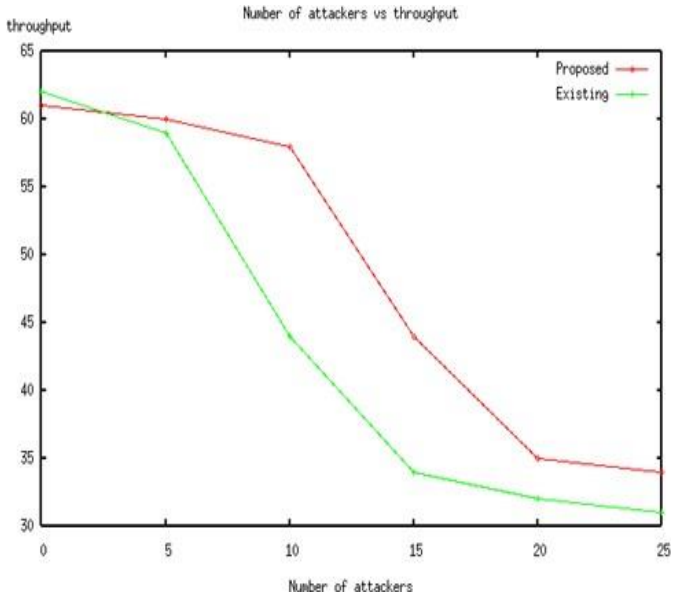

Figure.3 Attackers vs throughput

B) The Number of attackers vs. end-to-end delay

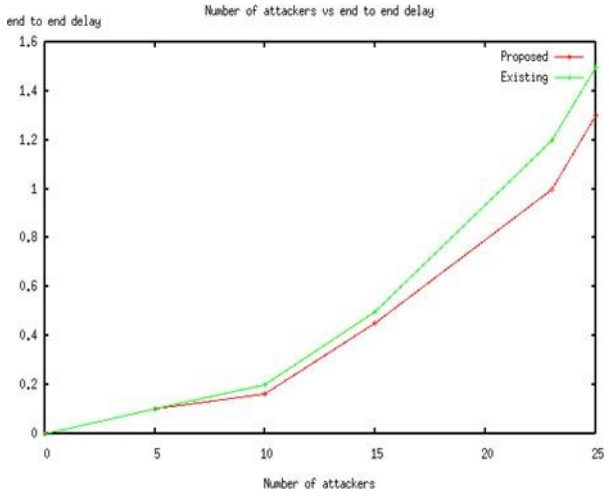

Figure.4 Attackers vs end to end delay

The graph, details the proposed mechanism is very competent than other the Existing scheme. In the Number of the attackers vs. the end-to-end delay, the graph explains at the time of increase in attacker, subsequently decreases the end-to-end based delay. Consequently, this paper concludes that projected system is extremely efficient one when compared to any of its existing method.

C) Number of nodes vs. packet delivery ratio

The above pictorial graph, relates the proposed methods is very effective when compared to Existing scheme. In the Number of nodes vs. the packet delivery ratio, the graph determines and suggests that when the number of nodes is increased then the packet delivery based ratio

also been increases. Therefore, this paper concludes with the proposed mechanism is very highly useful and enhanced when compared to that of the existing methods.

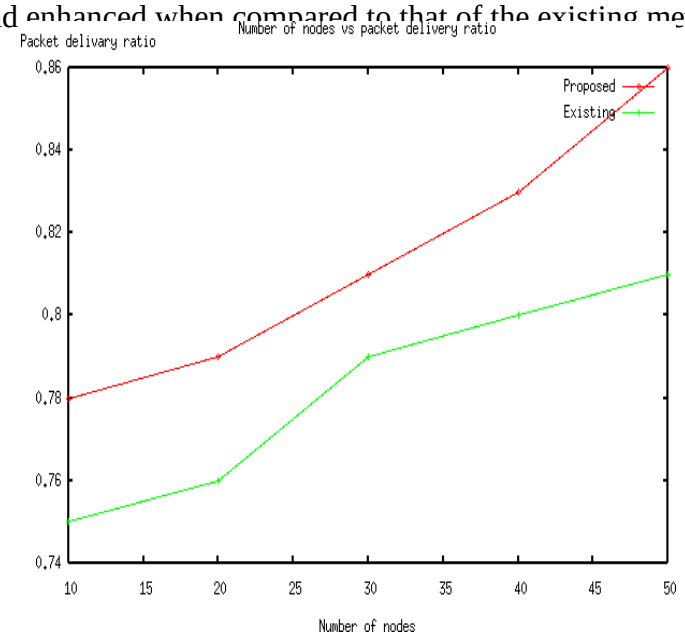

Figure.5 Number of Nodes vs Packet Delivery ratio

D) Number of nodes vs. Average Latency

The last and final comparison is made with as represented in the graph, that the proposed mechanism is very efficient when compared to the Existing methods. In the Number of the nodes vs. the Average latency, the graph denotes when the increase in number of the nodes then it automatically decreases the value of the Average latency. Therefore, this paper results that the projected scheme is highly effective when compared to that of the existing mechanism.

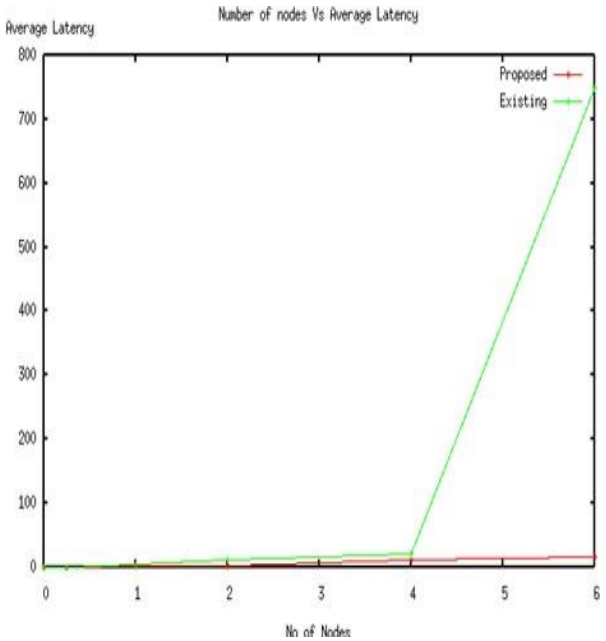

Figure.6 Number of Nodes vs Average Latency

Conclusions & Future Scope

The proposed method uses a role-oriented access control mechanism which combines the two approaches namely the cryptographic based primitives (i) A cryptographic based puzzle methods (ii) the key oriented cryptographic system. While a source node transmits a packet through these cryptographic based primitives, which all the nodes needs to institute a path or towards obtaining the packet, it will primary solves the puzzles following that it discovers the key for the decryption technique afterward only it be able to get the format of the original packet.

During this collective approach, the proposed method highly attains the very energy-efficiency, strong security, when compared to the existing scheme. The scheme performed numerous numerical studies as well as it is found that this proposed scheme of two- level based controller meet and achieves fast to the best solutions. This paper introduces a system with the design technique and the implementation of protocol with MNC and estimates its performance. The MNC technique fully explores the wireless based broadcast nature and the path diversity, that are taken into account while taking the advantage of the network coding that is to be adapted with its lossy based environment. With this highlighted salient properties that imitate in the distributed based algorithm which assign the broadcasting rate and the encoding to all the transmitters that has such properties, The MNC schemes attains a significant improvement in throughput over the traditional based routing and the existing network coding related protocols.

References

S. M. Metev and V. P. Veiko, *Laser Assisted Microtechnology*, 2nd ed., R. M. Osgood, Jr., Ed. Berlin, Germany: Springer-Verlag, 1998.

Akbar Batcha, Syed Musthafa, Securing data in transit using data-in-transit defender architecture for cloud communication, Soft Computing, springer, june 2021

Dr. A Syed Musthafa , M Praveenkumar ," E-agricultural system based intelligent predictive analysis and smart farming with digitalized demand and supply utilization to maximize the yield rate of crops using machine learning algorithm, Turkish Journal of Computer and Mathematics Education, Vol.12 No.10 (2021), pp 2036-2041

S. Zhang, C. Zhu, J. K. O. Sin, and P. K. T. Mok, ―A novel ultrathin elevated channel low-temperature poly-Si TFT,‖ *IEEE Electron Device Lett.*, vol. 20, pp. 569–571, Nov. 1999.

Dr. A. Syed Musthafa , C. Prashanth, "KIDNEY DISEASE DETECTION USING MACHINE LEARNING:, Turkish Journal of Physiotherapy and Rehabilitation; 32(2), ISSN 2651-4451, may 2021, pp 3359- 3365

M. Wegmuller, J. P. von der Weid, P. Oberson, and N. Gisin, ―High resolution fiber distributed measurements with coherent OFDR,‖ in *Proc. ECOC'00*, 2000, paper 11.3.4, p. 109.

R. E. Sorace, V. S. Reinhardt, and S. A. Vaughn, ―High-speed digital- to-RF converter,‖ U.S. Patent 5 668 842, Sept. 16, 1997.

M. Shell. (2002) IEEEtran homepage on CTAN. [Online]. Available http://www.ctan.org/tex- archive/macros/latex/contrib/supported/IEEEtran/*FLEXChip Signal Processor (MC68175/D)*, Motorola, 1996.

Syed Musthafa.A, "A Fuzzy based High-Resolution Multi-View Deep CNN for Breast Cancer Diagnosis through SVM Classifier on Visual Analysis", Journal of Intelligent & Fuzzy Systems, IOS Press, 10.3233/JIFS-189174, Page 1-14, September 2020

A. Karnik, ―Performance of TCP congestion control with rate feedback: TCP/ABR and rate adaptive TCP/IP,‖ M. Eng. thesis, Indian Institute of Science, Bangalore, India, Jan. 1999.

Syed Musthafa.A, Mohanraj.B, Priyanga.S, Krishnan.C, “High Security Distributed MANETs using Channel De-noiser and Multi-Mobile-Rate Synthesizer”, International Journal of Advanced Trends in Computer Science and Engineering, Volume 9, No. 2, ISSN 2278-3091, Page 1346- 1351, April 2020

J. Padhye, V. Firoiu, and D. Towsley, −A stochastic model of TCP Reno congestion avoidance and control,‖ Univ. of Massachusetts, Amherst, MA, CMPSCI Tech. Rep. 99-02, 1999.

Syed Musthafa A, Abdul Jaleel D, “Tourist Spot Proposal System Using Text Mining”, International Journal of Advanced Trends in Computer Science and Engineering, Volume 9, No. 2, ISSN 2278-3091, Page 1358- 1364, April 2020

Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification, IEEE Std. 802.11, 1997.