International Journal of Pure and Applied Mathematics
Volume 117 No. 15 2017, 725-742
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
Special Issue

ijpam.eu

WORMHOLE DETECTION USINGMULTIDIMENSIONAL SCALING WITH AES-CCM CRYPTOGRAPHY

K.P.Manikandan[1], Dr.R.Satyaprasad[2], Dr.Kurra.Rajasekhara Rao[3]

[1]*Associate Professor, IT Department,Dhanalakshmi Srinivasan College of Engineering,Coimbatore-641105, TN.*

[2]*CSE Department,Achariya Nagarjuna University,Nagarjuna Nagar-522510,AP.*

[3]*Professor in CSE & Director,Usha Rama College of Engineering and Technology,Telaprolu- 521109, AP.*

[1]manikandan_kp111@rediffmail.com , [2]profrsp@gmail.com, [3]krr_it@yahoo.co.in

ABSTRACT

As demand rises for universal network facilities, infrastructure-less and self-configuring systems like Mobile Ad hoc Networks (MANET) are gaining reputation. MANET routing securityhowever, is one of the most significant challenges to wide scale adoption, with wormhole attacks being an especially severe MANET routing threat.In this proposed method, the main objective is to provide secure data communication and also reduce malicious node present in the network.In this paper, Wormhole Detection using Multidimensional Scaling withAdvanced Encryption Standard -Cipher Block Chaining-Message Authentication Codecryptography (WDMSAC)technique is proposed that contain Multidimensional scaling methodwhich is applied in characteristics of extracted topology information to detect the wormhole attack. Advanced Encryption Standard -Cipher Block Chaining-Message Authentication Codecryptography(AES-CCM) is used in packet encryption thereby ensuring secure the packet transmission. In experimental result, analyze these existing and proposed techniques on the basis of their features that are vital task of detecting wormhole attacks in MANETs.

Keywords: Wormhole attack,WDMSAC technique, andMANET.

INTRODUCTION

Mobile *Ad hoc* Networks (MANET) are self-configuring arrangements of small portable devices interconnected by wireless links, with no fixed infrastructure like base stations and dedicated routers. They can be deployed in a diverse range of application domains, including wireless sensor and vehicular networks, military communications[1], and as a viable solution for Internet connectivity in *fourth-generation* (4G) networks, especially where nodes are located out of radio range, as for example in underground transport systems.Each MANET node participates

in the routing process, in addition to its other activities. A number of dedicated MANET routing protocols have been proposed, with the reactive protocols Ad hoc On-Demand Distance Vector (AODV) [2] and Dynamic Source Routing (DSR) [3], being the most widely adopted.

Openness of wireless communication channels, lack of any infrastructure and hostile environment where they may be easily deployed makes them vulnerable to various kinds of security attacks. There have been many researches on enhancing the security of mobile ad hoc networks. Especially, secure routing protocols have been developed in recent years. However, these researches only focus on the attacks by a single attacker[4].They have not considered the case of collusion attacks, in which multiple attackers cooperate with each other in order to exploit the received packets at the other area of networking. One attacker replays the packets that are forwarded from another attacker. These attackers can harm both the sender and thereceiver by dropping packets or illegally accessing thepackets. The wormhole attack is particularly challenging to detect as it can be mounted without compromising any of the nodes.

RELATED WORKS

TapodhirAcharjeeet. al.[5] in the year 2015 proposed a hybrid algorithm that can detect and prevent the wormhole attack and also wormhole link is successfully isolated from the concerned network. Jiu-huZhenget. al.[6] has proposed a different detection method which detects wormhole attacks with the connected relation of high connectivity nodes, and thereafteroptimizes routing with the help of the normal nodes outside the wormhole. This method has a better localization accuracy as it can well detect wormholes. NikiTsitsiroudiet. al.[7] proposed a visual-assisted tool to be developed for exposing security threats in IP enabled WSNs. The proposed tool, was named as called EyeSim, it is a user friendly, human-attractive visual-based anomaly detection system that is capable of alerting and monitoring the presence of wormhole links. The results show that it has the abilities to exactlynoticemany wormhole attacks in real-time. JuhiBiswaset. al.[8] proposed an algorithm WADP(Wormhole attack detection and prevention) algorithm by making modifications in the AODV routing protocol for detection and removal of wormhole attack in real-world MANET. The malicious nodes are detected using Node authentication. Node authentication is also used to remove the false positive problem that may arise in WADP algorithm, along with helping in mapping the exact location of the wormhole. Thus, it is a kind of double verification for wormhole attack detection. Megha

Sharma et. Al. [9] used an HMM driven approach, to be applied at an earlier stage of attack to identify the attacked wormhole tunnel pair.The attacked nodes areblocked and thereafter the preventive communication path isformed using fuzzy integrated communication analysis model.The network is simulated in NS2 environment.Ahmed Louazaniet. al.[10] presented a formal model using Time Petri Net to evaluate a proposed solution for detecting wormhole attack in Cross-Layer MAC protocol (CL MAC) in Wireless Sensor Networks(WSN). Meng-HsiuJaoet. al.[11] proposed a method to detect the wormhole attack without hardware equipment or requiring much information about WSN. A moving average (MA) indicator is used as a dynamic detection indicator of the number of neighbor nodes. The Quantum-inspired Tabu Search (QTS) algorithm is being used to arrange the numerous combinations. J. Anjuet. al. [12] proposed a detection technique for wormhole attack in MANET. This is accomplished in two phases. The preliminary or the first phase is the process ofdiscovering that a wormhole attack is done, it is based ontiming analysis and hop count. Once the attack has beensuspected, a Clustering based approach is used to confirm thepresence of attack, and also to identify the attacker nodes. The network is divided into various clusters and each cluster has a Cluster Head that controls all the nodes in the cluster and plays the role of a controlling authority in MANET.MostefaBendjimaet. al. [13] in order to achieve security and save ad hoc networks from attacks, a technique is proposed in which the network can be split into sectors, and Mobile Agents (MAs) are used to reject traffic intruders caused by Wormhole attacks considering the energy constraint.

PROPOSED METHODOLOGY

The main objective of this proposed work is to mitigate the vulnerabilities ofWormhole attacks which makeessential changes in the network topology. Wormhole attacks are identified by its distinctive topological characteristics of wormhole links.The proposed Multidimensional scalingis applied for detecting the wormhole attack. AES-CCMcryptography is used in packet encryption thereby ensuring secure the packet transmission. The main idea of detection approach is based on an observation as follows.

Wormhole attack detection Using Multidimensional scaling

Each node *v* in the network *G* collects its *k*-hop neighborhood information, in particular, $k = 2$. The sub graph is applied by MDS on the sub graph and embedding it on a plane. There are shortest distances (i.e., hop count) between all nodes pairs in the neighborhood sub graph $\lceil_G^k(v)$ are used to construct an estimation distance matrix. Then, the distance matrix isused to reconstruct be two conditions. First, if *v* is a normal node, the reconstructed sub graph would be relatively approximating to the original network. Thus, the embedded distance between each node pair is relatively close to their estimation distance. Otherwise, if *v* is a wormhole node, its 2-hop neighborhood sub graph contains all the wormhole nodes. Topologically, each wormhole node connectsto all nodes at the other end. Therefore, if it still embedded the subgraph on a plane, the distance constraints cannot be well maintained during the reconstruction. Based on this observation, let all nodes in the network perform local MDS-based reconstruction and detect potential Wormhole nodes according to the legality of their reconstructions. Additionally, introduces a simple and the effective necessary condition of wormholes to filter the suspect nodes detected by the previous process. Through this refinement process, we can remove most of false positives and identify all wormhole links.

Distance Estimation*:*

For an arbitrary node*v*in network *G*, it first collects its *k*-hop neighborhood information and obtains its *k*-hop neighborhood subgraph $\lceil_G^k(v)$. Next, a classical shortest-path algorithm, for example, Dijkstra's shortest path algorithm, is applied to calculate the shortest distances between all node pairs in $\lceil_G^k(v)$. Then, the shortest distance matrix *M* [$\lceil_G^k(v)$] is constructed, which is an *n*×*n* matrix (*n* denotes the number of nodes). Each element in M [$\lceil_G^k(v)$] is utilized as the estimation distance between each node pair.

Network Reconstruction:

Using the shortest distancematrix *M*[$\lceil_G^k(v)$] as input parameter, apply MDS to reconstruct the *k*-hop neighborhood subgraph of *v*. MDS denotes the reconstructed network by $\lceil_G^k(v)$, in which each node assigned a virtual position (i.e., node coordination's). Then, the Euclidian distance between eachnode pair is calculated in $\lceil_G^k(v)$, and a virtual distance matrix[$\lceil_G^k(v)$] is produced.

Wormhole Judgment:

Then, it describes how to decidewhether a node is a wormhole node candidate by its reconstructed neighborhood subgraph. First, the distortion factor of the MDS reconstruction is calculated for each nodeB.The distortion factor is defined as follows.

Definition 1 (distortion factor). The distortion factor$\lambda(v)$is defined as the Root Mean Square Error (RMSE) between the shortest distance matrix $M[\ulcorner^k_G(v)]$ and the recon-Strutted virtual distance matrix $M[\ulcorner^k_G(v)]$, that is,

$$\lambda(v) = \sqrt{\left(\frac{1}{n \times n}\right)\sum_{i=1,j=1}^{n}(M[\ulcorner^k_G(v)](i,j) - M[\ulcorner^k_G(v)](i,j))^2}$$

As discussed previously, each node produces large distortion factor if it is a wormhole node and a little distortion factor otherwise. Based on this observation, set a predefined threshold and label nodes,that produces distortion factors above this threshold as suspect wormhole nodes. In our experiment, we set the threshold to be the median value of the distortion factors of all nodes in G, that is, $\lambda_{threshold} = \lambda_{max} + \lambda_{min})/2$ and $\lambda_{max} = \max\{\lambda(v): v \in V(G)\}, \lambda_{min} = \min\{\lambda(v): v \in V(G)\}$ respectively.

Then, we present an efficient way to generate the threshold and distribute it to all nodes. Each node floods a message that contains its distortion factor and records the maximum and minimum values of all distortion factors in all flooding messages it receives. Each node only relays messages that contain a new maximum or minimum value. Thus, only two messages that, respectively, contain the globalmaximum and minimum values flooded to the whole network. After the flooding is finished, each node calculates the threshold from the maximum and minimum values it records and compares it with its own distortion factor. If its distortion factor exceeds the threshold, it is labeled as a suspect wormhole node and normal node otherwise.After the implement of this component, a number of suspect wormhole nodes are produced.

Wormhole Detection Algorithm using Multi Terms and Scaling.

Input:
A network graph $G(V, E)$.
Output:
A set of complete bipartite graphs B.
(1)**for** each$\boldsymbol{v \in V\ do}$

(2) Collect *k*-hop neighborhood subgraph $\lceil_G^k(v)$.
(3) Calculate the shortest distance matrix *M* [$\lceil_G^k(v)$].
(4) Reconstruct the subgraph by MDS.
(5) Calculate the virtual distance matrix *M* [$\lceil_G^k(v)$].
(6) Calculate the distortion factor$\lambda\ (v)$.
(7) Flood $\lambda\ (v)$ to the network.
(8) Calculate the threshold$\lambda_{threshold}$.
(9) **if** $\lambda_v > \lambda_{threshold}$ **then**
(10) Add *v* to the suspect node set *S*.
(11) **end if**
(12) **end for**
(13) Find all connected components C from *S*.
(14) **for** each$\boldsymbol{c \in C\ do}$
(15) Find each MCBS *B* from *C*.
(16) Add *B* to the MCBS set B.
(17) **end for**
(18) **for** each $B = \{X, Y\}$ inB **do**
(19) **if** $N_G^k(X) \cap N_G^k(Y) = \emptyset$ **then**
(20) Remove edges $X \times Y$.
(21) **else**
(22) Remove *B* from B.
(23) **end if**
(24) **end for**

AES-CCM ALGORITHM

Advanced Encryption Standard [14] is a standard is identified for a symmetric block cipher mechanism which uses 128 bits, 192 bits, and 256 bits of key sizes. CCM is an Authenticated Encryption Standard which is built on a key management assembly. In this algorithm the plain text is separated into block ciphers of 128 bits size. The means of operation used in the AES-CCM is counter means (CTR) with Cipher Block Chaining and Message Authentication Code (CBC-MAC). They make a generation-encryption and decryption-verification functions [15]. The privacy feature is done in the CTR method by AES and the verification is done in CBC-MAC with the MAC value created. In AES-CBC-MAC, the encryption purpose is practical to the first block to generate a cipher. Then cipher results as XO Red with the next block to obtain the following result. The method has been going on for all the

outstanding blocks until the last value MAC is found, it is used in CTR mode encryption. The following 3.1 shows the block diagram of AES-CBS-MAC.

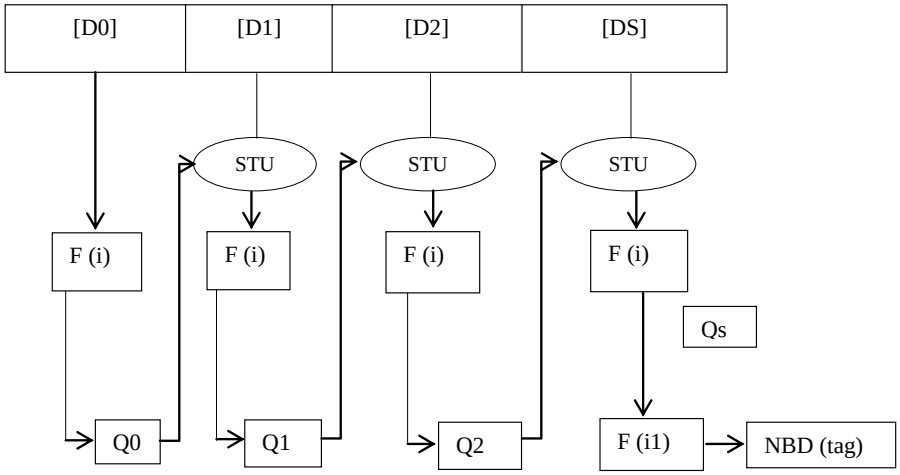

Figure: 1 Block diagram of AES-CBC-MAC

In AES-CTR, alternative cipher blocks are formed which are dependent on nonce worth. The CTR mode is functioned to MAC and the payload to attain the cipher-text. CCM is not companionable with steam ciphers and it will not work with the Data Encryption Standard which supports 64 bits of the block.

The input features of CCM are: the effective payload ($pd > 2\hat{}64$)(The data is authenticated and encrypted), the effective nonce ($nc < 2\hat{}61$) (must be unique), and the effective linked data ($ad \leq 256\ bits$) (authenticated but not encrypted). The nonce is practical to the payload and linked data. The secret key (*k*) to the block cipher which is generated evenly at casual whose size is 128 bits. CCM only works with the advancing cipher function [15].

A. Generation-Encryption

In Generation-Encryption mechanism, cipher chunk attaching is practical to the payload (*pd*), the nounce (*nc*) and the associated data (*ad*) to generate MAC. The MAC length (*Mlen*) is

continuously greater than or equal to 64 bits. Then the counter method encryption is practical to the MAC and payload to change it into cipher text [15].

Prerequisites:

The numerous Prerequisites are essential are as follows; the cipher block algorithm, key *k* counter generation function, formatting function MAC length *Mlen*.

Input:

The input principles are essential: valid payload pd of length pdlen bits, valid association data ad; valid nonce nc.

Output:

The output of a cipher –text C.

Steps:

1. *Put on the planning purpose to (nc,ad,pd) to create the blocks D0, D1,…Dr*
2. *Set W0=CIPHk(D0)*
3. *For H =1 to s, do Wh=CIPHj(Dh EFG Wh-1)*
4. *Ste MAC=MSBMlen (Ws)*
5. *Apply the counter generation function to generate the counter blocks PQSO, PQS1,….PQSn, where m=pdlen/128*
6. *For e=0 to n, do er=CIPHr(PQSr)*
7. *Set* $T = T1\|T2\| \ldots . \|Tm$
8. *Return* $B = (pd\ EFG\ MSB\ pdlen\ (s))\|(MAC\ EFG\ MSB\ Mlen\ (T0))$

B. Decryption-Verification

In decryption verification mechanism, counter mode decryption is done to get the MAC worth and its equivalent payload.Cipher block chaining is functional to the payload, the nonce received, and the allied data received to check if the MAC is right.If the certification succeeds it means that input are created from the foundation and have access to the key.MAC

acts the most vital role as it can keep away safekeeping threats and can safeguard data from being improved.

Prerequisites:

The various Prerequisites that are required are: Cipher block algorithm; Key k; Counter generation function; Formatting function; and Valid MAC length Mlen.

Input:

The foremost input significance is: association data, ad; valid nonce, nc; cipher text C of length cplen bits.

Output:

The output will be any payload pd or INVALID

1. *If* $Cplen \leq Mlen, then\ return\ INVALID$
2. Put on the counter generation function to create the counter blocks PQS0, PQS1… PQSi
3. *For* $e = 0\ to\ i, do\ R_e = CIPH\ k(PQSi)$
4. *Set* $R = R1 \| R2 \| \ldots . \| Ri$
5. *Set* $pd = MSB\ cplen - Mlen\ (C) STU\ \ MSB\ cplen - Mlen(S)$
6. *Set* $MAC = LSB\ Mlen\ (C) STU\ MSB\ Mlen\ (S0)$
7. If nc, ad or pd is not effective, then return INVALID, else apply the planning purpose to (nc, ad, pd) to create the blocks $F_0, F_1, \ldots \ldots, F_r$
8. *Set* $T0 = CIPH\ j(F)$
9. *For* $H = 1\ to\ r. do\ W_e = CIPH(F_n\ STU\ W_{n-1})$
10. If $MAC \neq MSMBlen(W_f), then\ return\ INVALID, else\ return\ pd$

EXPERIMENTAL RESULT AND DISCUSSION

The proposed model for the detection of wormhole nodes in a network is analyzed through the ns2 simulator tool. The version ns2.34 tool is mainly used for the simulations of MANET, VANET, WSN and so forth. The Proposed WDMSAC techniques of parameters such

as a true negative ratio, average delay, PDR, routing overhead, detection ratio and false detection ratio is compared with existing algorithms namely PAP and SCF[16] cluster. Table 1 shows that simulation parameter of proposed work.

Table 1. Simulation Parameter

Simulation Parameter	Value
Propagation	Two Ray Ground
Channel	Wireless Channel
Physical Layer	Wireless Physical
Queue	Drop Tail/PriQueue
Mac	802_.11
X dimension of the topography	500
Y dimension of the topography	500
Ad hoc Routing	AODV
Antenna	Omni Antenna
Max packet	100
Number of nodes simulated	100
Cp	./cbr
Sc	nodes50
Simulation time	100 s
Energy	Energy Model
Initial Energy	100
MinNeighbor	6
SecurityDuration	4
Adversary node	5

AlgorithmsWDMSAC compared with ECC_SCF_PAP, PAP and SCF cluster that is shown in the following graph.

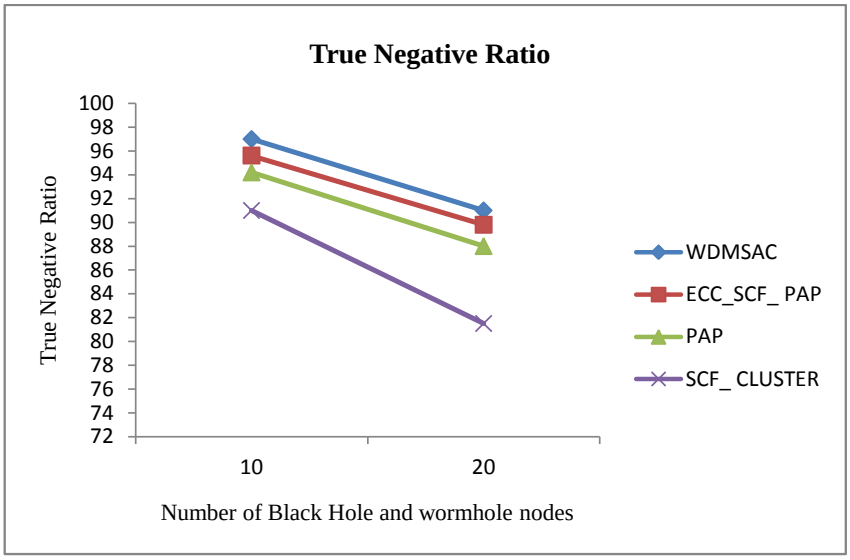

Figure: 2 Graph of True negative ratio

True negative ratio measures the ratio of negatives that are correctly identified. Therefore the percentage of node which are correctly identified as not under the false condition.

$$True\ negative\ ratio = \frac{TN}{TN + FP}$$

Where True negative (TN) value is the number of correctly identified as non-malicious node and False positive (FP) value is the number of correctly identified as malicious node.

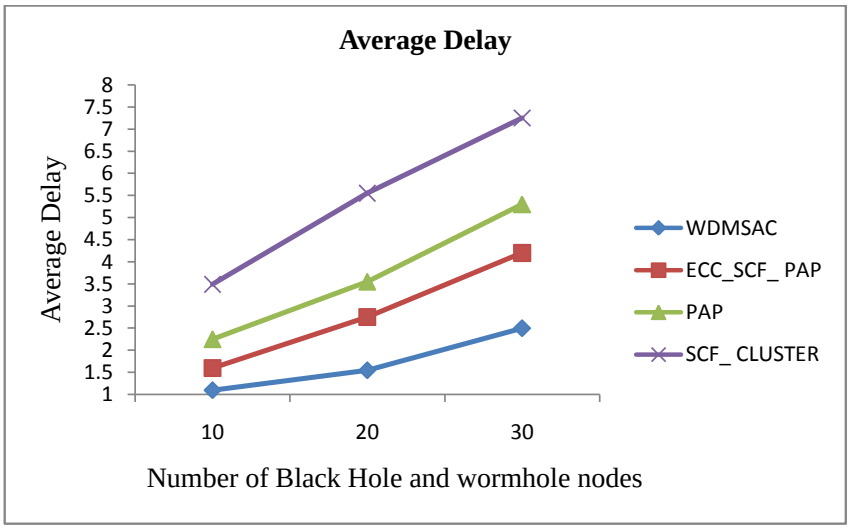

Figure: 3Graph of average delay

The average delay is the parameter which reflects the usage degree of network resources for routing protocols. It is given in seconds.This can be calculated as the summation of all delay samples to the total number of samples.

$$Average\ delay = \frac{Sum\ of total\ packet\ delay}{Total\ number\ of\ received\ packets}$$

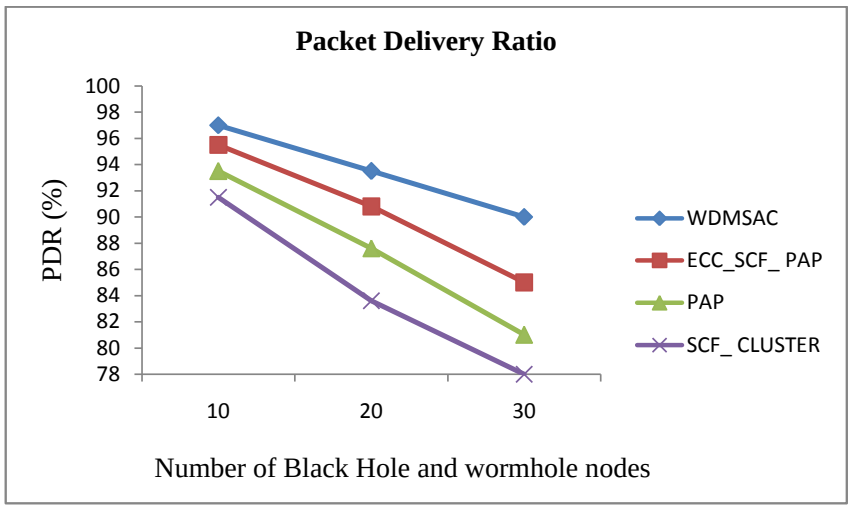

Figure: 4 Graph of PDR

Packet Delivery Ratio (PDR) is the ratio between the number of packets, delivered by a traffic source node and the number of packets acknowledged by a traffic drop. It measures the loss rate as seen by transport protocols, and it describes both the rightness and effectiveness of mobile ad hoc routing protocols.

$$PDR = \frac{Packets\ received}{Packets\ Deliverd} \times 100$$

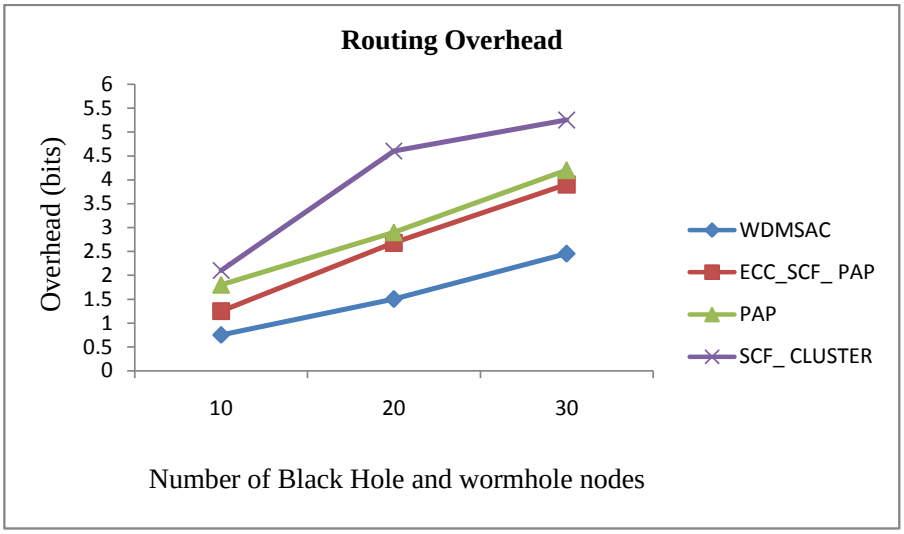

Figure: 5 Graph of routing overhead

Routing overhead is the percentage of packets generated for routing and packets received at the destination. Its value is given in bits. Routing overhead is the amount of routing control packets in circulation in the network where these are responsible for route discovery and route management.

$$\text{Routing overhead} = \frac{Total\ number\ of\ Routing\ packets\ transmitted}{a\ data\ packet\ sent\ to\ destination}$$

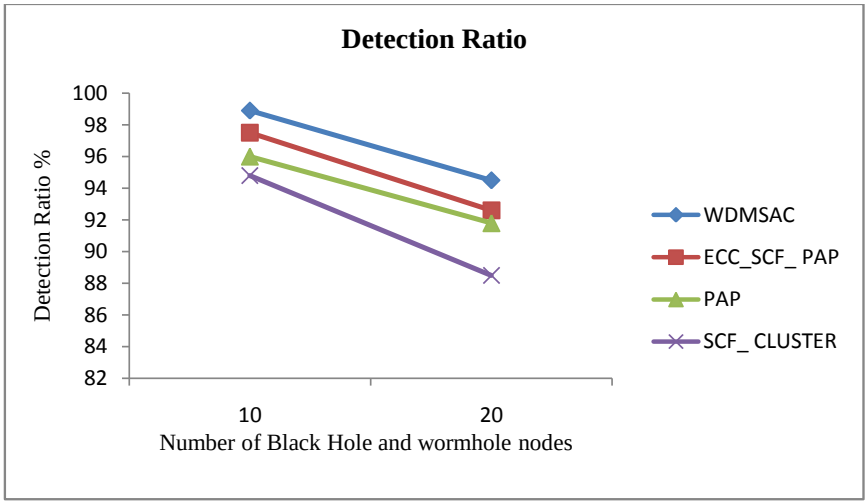

Figure: 6 Graph of detection ratio

This is the ratio of finding of malicious node among all nodes in the network. It is calculated in percentage of detection ratio. The detection ratio increases with decrease in mobility because the changes are less on routing table and thus it is ease to identify abnormal behavior. In case if mobility is high, the detection ratio is low respectively.

$$\text{Detection ratio} = \frac{\text{sum of ratio of routing packets } [\text{sent data packets} - \text{received data packets}]}{average\ of\ data\ packets\ delivered}$$

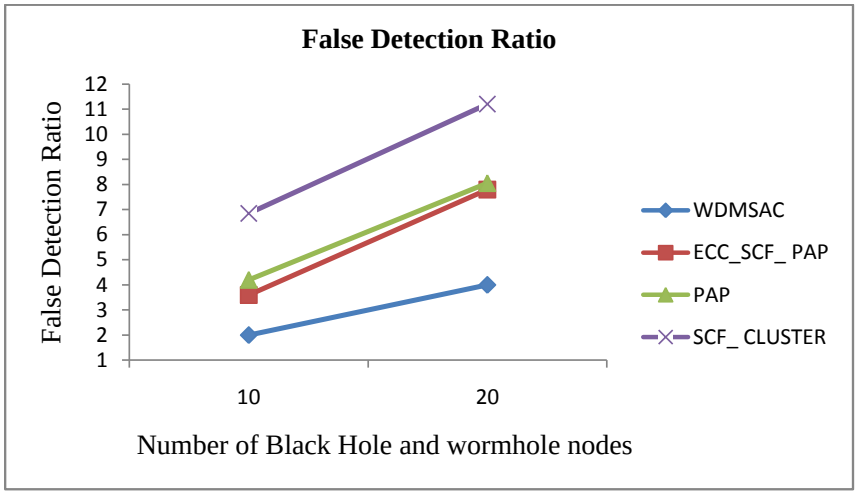

Figure: 7 Graph of false positive ratio

It is the percentage of decision in which normal notifications are flagged as unusual problem. Through, these analyses of probability of aggregated routing control packet source address, the sudden, unexpected changes yet normal activate are eliminated.

$$\text{False positive ratio} = \frac{\text{False discovery of malicious node}}{total\ number\ of\ discoveries}$$

The metric values are tabulated as follows:

Table 2 (a): Performance analysis of True Negative, Detection and False detection ratio

Number of black hole and wormhole nodes	True Negative Ratio				Detection Ratio				False Detection Ratio			
	WDMSAC	ECC_SCF_ PAP	PAP	SCF_ CLUSTER	WDMSAC	ECC_SCF_ PAP	PAP	SCF_ CLUSTER	WDMSAC	ECC_SCF_ PAP	PAP	SCF_ CLUSTER

10	97	95.6	94.2	91	98.9	97.5	96	94.8	2	3.6	4.2	6.85
20	91	89.8	88	81.5	94.5	92.6	91.8	88.5	4	7.8	8.05	11.2

Table 2 (b): Performance analysis of Average delay, PDR and Routing Overhead

Number of black hole and wormhole nodes	Average Delay				PDR				Routing Overhead			
	WDMSAC	ECC_SCF_ PAP	PAP	SCF_ CLUSTER	WDMSAC	ECC_SCF_ PAP	PAP	SCF_ CLUSTER	WDMSAC	ECC_SCF_ PAP	PAP	SCF_ CLUSTER
10	1.1	1.6	2.25	3.49	97	95.5	93.5	91.5	0.75	1.25	1.8	2.1
20	1.55	2.75	3.55	5.55	93.5	90.8	87.6	83.6	1.5	2.68	2.9	4.6
30	2.5	4.2	5.3	7.25	90	85	81	78	2.45	3.9	4.2	5.25

CONCLUSION

Openness of wireless communication channels, and the nature of hostile environment where theattackers can easily deploy vulnerable activities which make various kinds of security attacks. In this paper, Wormhole Detection using Multidimensional Scaling with AES-CCM cryptography (WDMSAC) technique is proposed to detect the wormhole attack. In experimental result, the detection of black hole and wormhole attack nodes in the network is efficiently detected using this proposed algorithm model.

REFERENCES:

1. Jonny Karlsson, Laurence S. Dooley,and GöranPulkkis, “A New MANET Wormhole Detection Algorithm Based on Traversal Time and Hop Count Analysis”, Sensors (Basel), Vol,11, no.12, pp.11122-11140, 2011.

2. Perkins C.E., Royer E.M."*Ad-Hoc* On-Demand Distance Vector Routing", Proceedings of the Second IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'99); New Orleans, LA, USA. pp. 90–100,February 1999.
3. Johnson D.B., Maltz D.A." Dynamic Source Routing in *Ad Hoc* Wireless Networks", Mobile Computing, Kluwer Academic Publishers,Vol. 353, pp. 153–181,1996.
4. JuhiBiswas1 , Ajay Gupta2 , Dayashankar Singh, "WADP: A Wormhole Attack Detection And prevention Technique in MANET using Modified AODV routing Protocol", 9th International Conference on Industrial and Information Systems (ICIIS), IEEE,pp.1-6, 2014.
5. TapodhirAcharjee; Pinky Borah; Sudipta Roy, "A New Hybrid Algorithm to Eliminate Wormhole Attack in Wireless Mesh Networks", International Conference on Computational Intelligence and Communication Networks (CICN),2015.
6. Jiu-huZheng; Huan-yanQian; Lei Wang, "Defense Technology of Wormhole Attacks Based on Node Connectivity", IEEE International Conference on Smart City/SocialCom/SustainCom (SmartCity),2015.
7. NikiTsitsiroudi; PanagiotisSarigiannidis; EiriniKarapistoli; Anastasios A. Economides, EyeSim: A mobile application for visual-assisted wormhole attack detection in IoT-enabled WSNs at 9th IFIP Wireless and Mobile Networking Conference (WMNC) (2016)
8. JuhiBiswas, Ajay Gupta, Dayashankar Singh, WADP"A wormhole attack detection and prevention technique in MANET using modified AODV routing protocol" , 9th International Conference on Industrial and Information Systems (ICIIS),2014.
9. Megha Sharma; Ajay Khunteta; Deepak Sharma "Fuzzy integrated HMM model for communication optimization underwormhole attack in mobile network ",International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT),2015
10. Ahmed Louazani, LarbiSekhri, BouabdellahKechar" A time Petri net model for wormhole attack detection in wireless sensor networks", International Conferenceon Smart Communications in Network Technologies (SaCoNeT),2013
11. Meng-HsiuJao; Ming-Hsuan Hsieh; Kuan-Hsien He; Dai-Hua Liu; ShuYuKuo;Ting-Hui Chu; Yao-Hsin Chou " A Wormhole Attacks Detection Using a QTS Algorithm with MA in WSN", IEEE International Conference onIn Systems, Man, and Cybernetics (SMC), Pg:20 – 25, 2015.

12. J. Anju, C. N. Sminesh: An Improved Clustering-Based Approach for Wormhole Attack Detection in MANET,3rd International Conference on Eco-friendly Computing and Communication Systems (ICECCS), 2014.
13. MostefaBendjima, Mohammed Feham "Wormhole attack detection in wireless sensor networks", SAI Computing Conference (SAI) , Pg: 1319 – 1326,2016.
14. Daemen, Joan; Rijmen, Vincent ,"AESProposal: Rijndael", National Institute of Standards andTechnology, February 2013.
15. Morris Dworkin , "Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality", National Institute of Standards and Technology Special Publication 800-38C Natl. Inst. Stand. Technol. Spec. Publ. 800-38C 25 pages (May 2004).
16. Nageswaran.C.M and Faizal Mukthar Hussain.S "Cluster Based MANET of Self Node Detection in SCF+ Tree" International Journal of Innovations in Scientific and Engineering Research (IJISER) ,Vol 2, Issue 4,pp.93-98, 2015
17. Rajesh, M., and J. M. Gnanasekar. "Annoyed Realm Outlook Taxonomy Using Twin Transfer Learning." International Journal of Pure and Applied Mathematics 116 (2017): 547-558.
18. Rajesh, M. & Gnanasekar, J.M. Wireless Pers Commun (2017),https://doi.org/10.1007/s11277-017-4565-9
19. Rajesh, M., and J. M. Gnanasekar. "GCCover Heterogeneous Wireless Adhoc Networks." Journal of Chemical and Pharmaceutical Sciences (2015): 195-200.
20. Rajesh, M., and J. M. Gnanasekar. "CONGESTION CONTROL IN HETEROGENEOUS WANET USING FRCC." Journal of Chemical and Pharmaceutical Sciences ISSN 974: 2115.
21. Rajesh, M., and J. M. Gnanasekar. "GCCover Heterogeneous Wireless Ad hoc Networks." Journal of Chemical and Pharmaceutical Sciences (2015): 195-200.
22. Rajesh, M. "Object-Oriented Programming and Parallelism."
23. Rajesh, M., K. Balasubramaniaswamy, and S. Aravindh. "MEBCK from Web using NLP Techniques." Computer Engineering and Intelligent Systems 6.8: 24-26.