Wormhole Attack Detection and Prevention Using EIGRP Protocol Based on Round Trip Time

K. Karthigadevi[1,*], S. Balamurali[1] and M. Venkatesulu[2]

[1]*Department of Computer Applications, Kalasalingam Academy of Research and Education, Krishnankoil 626 126, Tamilnadu, India*
[2]*Department of Information Technology, Kalasalingam Academy of Research and Education, Krishnankoil 626 126, Tamilnadu, India*
E-mail: k.karthikrish@gmail.com
**Corresponding Author*

Received 11 January 2018; Accepted 07 May 2018;
Publication 12 June 2018

Abstract

One of the major harmful attacks in wireless sensor network is wormhole attack. These attacks are disturbing the routing in networks and create a large amount of traffics. Wormhole attacks are target to the banks, government, private sectors, public sectors etc. The proposed method is used to analyse and detect the wormhole attack. Using EIGRP protocol to identify the shortest path and detect the attacking node based on the round trip time variation technique. As compared with previous method, it is the easy way to detect the wormhole attacks.

Keywords: WSN, Wormhole attack, RTT, EIGRP, Intruder node.

1 Introduction

A sensor node in a network is used to perform some processes, gather sensory information and transfer it with other associated nodes in the network. A wireless sensor network (WSN) consists of some of the independent sensor

Journal of Cyber Security and Mobility, Vol. 7_1, 215–228. *River Publishers*
doi: 10.13052/jcsm2245-1439.7115

devices which are used to monitor the physical and environmental conditions. This system includes a gateway that provides wireless connectivity back to the wired world and distributed nodes.

1.1 Attacks on the WSN

A number of attack is available in WSN like, Black hole attacks, black mail attacks, Gray hole attack, Traffic Analyze Attack, wormhole attack etc [21].

1.2 Wormhole Attack

An affected node can accept the packets from neighbour node and transfer it into some other location. This wormhole attack is one of the most harmful attacks which can easily affect the network without having any awareness of the legitimate nodes. Intruder can forward each bit instead of waiting for the whole packet to create wormhole for packets not addressed to self and the wormhole attack can be performed even when communication is confidential.

1.3 Enhanced Interior Gateway Routing Protocol

Enhanced Interior Gateway Routing Protocol (EIGRP) is one of the advanced routing protocols. It is used to determine the best path to the destination. It operates on the large networks with higher efficiency and each router maintains the topology table. It is useful for the reliable communication in the network.

2 Literature Survey

Ronghui et al. [1] proposed a Beacon Method which provides very low localization error, and low calculation cost and this method is valid only for layered architecture of the network. Chen et al. [2] established the concept of the secured location approach based on the wormhole attack and also conflicting set [3] based on the wormhole detection. Distance consistency based secure location is used for the prevention of the attacks. In this method, more number of packets are loss. Conflicting set method is used for filtering the incorrect distance measurement in adjacent locators.

Graph theoretical method has been proposed by the Lazos et al. [4]. Encryption method is used to detect and prevent wormhole attacks. Otero et al. [5] proposed the wormhole attack detection in WSN with the range-free localization. Here Routing protocol is used to detect the wormhole attack. Range free localization method can be used only for the out-of band channel.

Statistical method based detection has been proposed by the Vajda et al. [6]. Neighbour number test and all distance tests can be used to detect the wormhole attack.

Song et al. [7] introduced a new scheme based on statistical analysis of multi path. The maximum relative frequencies are used to detect the wormhole attacks. Hop count and the delay per hop indication methods are used for the detection of the wormhole attacks [8]. In this method, alarm is not detected and also rescheduling of the packets is very high. Sharif et al. [9] proposed the wormhole detection based on the Ad-hoc networks. In this method, demand routing protocol and secure neighbour detection protocol are used for not only to detect the wormhole link but also to provide a verification mechanism to judge the validity of nodes.

Introducing intuitive method has been proposed by Jen et al.[10] to detect and prevent the wormhole attack in MANET. This method provides a high efficiency compared with the existing methods and also has good performance with low overhead. Since wormhole attacks are simple to apply but very hard to identify, in this paper EIGRP protocol based on round trip time is used to detect and prevent the wormhole attack.

Arun Prakash et al. [11] selected a proper leader to mitigate the wormhole attack by using coordinators algorithm, which is used to find the correct path to transfer the data and detect the wormhole attack. Parvinder Kaur et al. [12] developed a novel algorithm which can be used to detect the wormhole attack and is also used to reduce the end to end delay calculation for two nodes with in a communication range.

Aaditya Jain et al. [13] used RTT and Modified Wormhole Detection AODV protocol (MAODV) method to detect and prevent the wormhole attack. Gu-Hsin Lai et al. [14] the node rank will be identified using RPL technique (Routing Protocol for Low-Power and Lossy Networks). The unreasonable node will be declared as a malicious node and detect it.

Rahul Jain et al. [15] detected the wormhole attack to create a sequence number and secure path to transfer data from source to destination. Shiyu Ji et al. [16] developed detection algorithm which can be used to detect the wormhole attack and improve the efficiency of the network. Manish Patel et al. [17] detected the wormhole attack based on neighbourhood and connectivity constraints and also reduce the storage cost of the wormhole attack.

Mostefa Bendjima et al. [18] split the network in to sectors and mobile agents to identify the wormhole attack. Using SINALGO simulator to detect the wormhole attack. Nivedha et al. [19] compared existing methods and detect

the wormhole attack during data transmission. Akansha Shrivastava et al. [20] summarized various detection techniques like Distance and location based approach: geographical and temporal, Directional Antenna, LITEWORP etc.

3 Detection and Prevention of Wormhole Attack

To find out multiple paths between the source and the destination, the EIGRP which is an extension of IGRP protocol is used. In EIGRP routing protocol, it is first checked whether, the route is available or not for two way communication. If the route is available then the RREQ packet is send to its successor. When the receiver gets the RREQ packet then it sends out RREP packet to the starting place along with the same path to RREQ packet. Likewise RREQ, packets arrived from all other directions to RREP packets are forwarded via the same path. All the routing paths are stored at the source node. This protocol easily calculates the neighbour node.

Proposed method is used to detect the wormhole attack using EIGRP protocol. RREQ packet is send from the starting node on that time is Rt1 and also set the time of the RREP packets. Multiple acknowledgements are received from the destination node means to fix the times Rt2_i of each RREP packets. RTT Rt3_i values are getting from the Rt1 and Rt2.

Based on the Round Trip Time of Rt3_i, compute the average RTT of all the paths with the help of the value Rts_i. After comparison of the threshold value of Round Trip Time Rts_i, check whether the total round trip time is less than threshold round trip time Rt^{th} or not and the hop count of particular route is equivalent to two or more than the wormhole link, then that route is affected by wormhole otherwise no threat is occurred in that wormhole link. Once the wormhole link is identified in that direction, then sender fixes that node W1 as wormhole node and forward false RREQ packet through that particular route i and successor W1 node. The destination gets false RREQ packet from its successor W2 and detect that W2 node as wormhole node. The nodes W1 and W2 are removed from the network. Then automatically wormhole affected link is blocked. The further transaction between source and destination nodes routes are first checked in the routing table. If the route found to have any wormhole link then it will not take that direction instead it will take another direction to transfer the packets from source to destination. Benefits of using EIGRP is faster converging because it pre calculates routes and does not broadcast hold-down timer packets before converging.

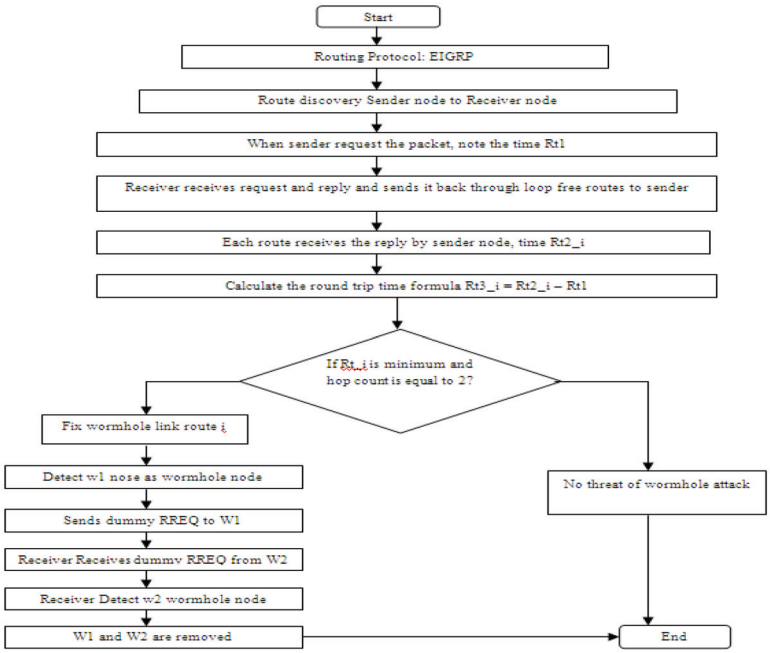


Figure 1 Flow chart of the proposed algorithm.

3.1 Algorithm

Step 1: Start
Step 2: Set time Rt1.
Step 3: Sender node time Rt2_i
Step 4: Calculate Round Trip time formula
Rt3_i = Rt2_i – Rt1.
Step 5: Calculate Round Trip Time threshold value formula

$$\text{Rts\_i} = \frac{Rt3\_i}{hop\ counti}$$

Step 6: Find average Rts_i
Step 7: Find threshold round trip time Rtth for each route

$$\text{Rts\_1} = \frac{Rt3\_1}{hop\ count1}, \quad \text{Rts\_2} = \frac{Rt3\_2}{hop\ count2}, \quad \text{Rts\_3} = \frac{Rt3\_3}{hop\ count3}.$$

Step 8: If Rts_i $<$ Rtth and hop count[i] $= 2 =$ true then

i. Fix route i as wormhole link
ii. Sender fix successive node W1 as wormhole node
iii. Sender sends dummy RREQ to W1
iv. Receiver receives dummy RREQ from its successive W2
v. Receiver fix W2 as wormhole node
vi. W1 and W2 are removed and broadcast to other nodes

Step 9: otherwise there is no threat of Wormhole attack
Step 10: End

3.2 Simulation and Results

In Figure 2, the Packets is transferred from source node S to destination node D. The in between nodes are A, B, C, F and E. Two possible paths to transfer the packets from node S to D are

i. S-A-B-C-D
ii. S-F-E-D

Consider the E-D link is wormhole attack link. So the wormhole attack nodes are E and D.

3.3 Transaction

Table 1 specifies the time, packet transaction between two nodes, packet transmission time and acknowledgement time. Comparing the time T4 to other times like T1, T2 and T3, there is no time delay for transmission time and the acknowledgement time. In time T4, when the node E – D transfer the packets it takes long time to send acknowledgement.

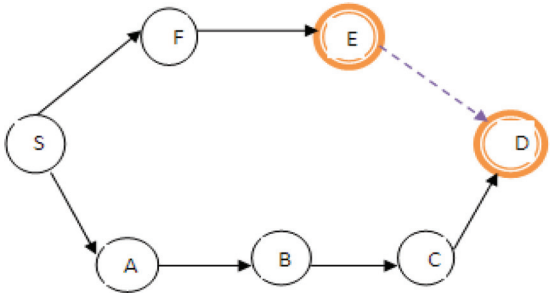


Figure 2 Packet transmission flow diagram.

Table 1 Transmission time between Packets

Time	Packet Transaction	Transmission Time	Acknowledgement Time
T1	S – A	12:20:30	12:21:25
	S – F	12:20:30	12:23:10
T2	A – B	12:23:15	12:23:50
	F – E	12:23:15	12:24:52
T3	B – C	12:24:15	12:24:40
	E – D	12:24:15	12:50:10
T4	E – D	12:50:50	01:20:50
	C – D	12:50:50	–
T5	E – D	01:25:10	–
	C – D	–	–

3.4 Calculation

Table 2, shows delay time calculation which is performed based on node transmission.

Delay time = Acknowledgement time – Request time. When the packets are transferred from E – D, it takes more time and also the further transaction will not be performed. So E – D link is a wormhole attack link. To confirm whether the link is really a wormhole link, to send fake RREQ packets to that particular link E – D. If the wormhole attack is affected by this link, the nodes is never send acknowledgement. Other nodes are waiting for the RREP msg.

Table 3 shows the simulation results which are based on delivery rate, average end to end delay and average throughput by comparing normal EIGRP protocol and wormhole affected EIGRP protocol. Initially take 10, 20, 30, 40 and 50 nodes respectively.

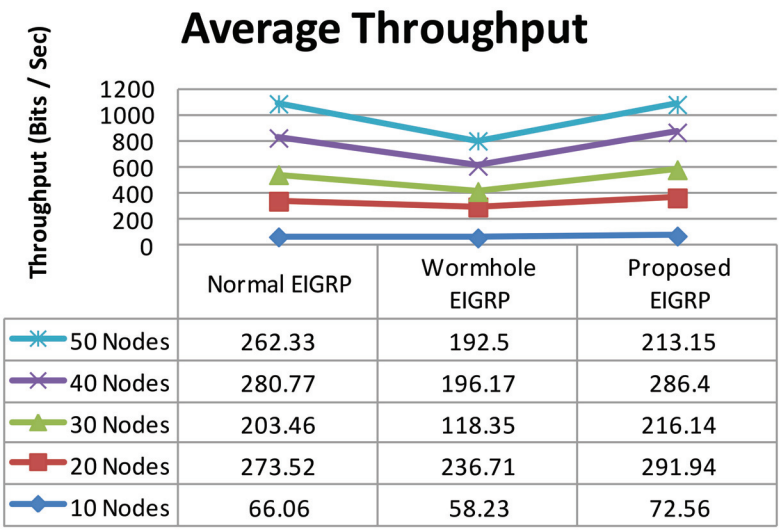
In Figure 3., the proposed EIGRP increases the values of the throughput. Throughput is the rate of packets received at the destination successfully. It is

Table 2 Delay time calculation

Time	Node Transmission	Delay Time
T1	S – A	0 : 1 : 35
	S – F	0 : 5 : 01
T2	A – B	0 : 0 : 58
	F – E	0 : 2 : 28
T3	B – C	0 : 0 : 42
	E – D	0 : 43 : 25
T4	E – D	1 : 60 : 34
	C – D	–
T5	E – D	–
	C – D	–

Table 3 Simulation factor

S.No	Constraints	Value
1	Simulation area	500m × 500m
2	Routing Protocol	EIGRP
3	Packet volume	512 bytes
4	Traffic Rate	CBR(Constant Bit Rate)
5	Number of Nodes	10, 20, 30, 40 and 50
6	Range Transmission	230m
7	Simulation time	200s
8	Mobility model	Fixed

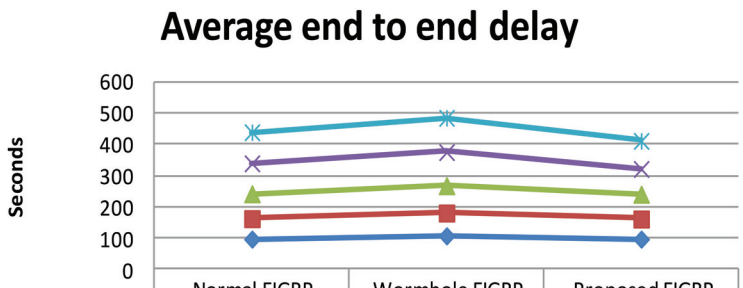


	Normal EIGRP	Wormhole EIGRP	Proposed EIGRP
50 Nodes	262.33	192.5	213.15
40 Nodes	280.77	196.17	286.4
30 Nodes	203.46	118.35	216.14
20 Nodes	273.52	236.71	291.94
10 Nodes	66.06	58.23	72.56

Figure 3 Average throughput for 10, 20, 30, 40 and 50 nodes.

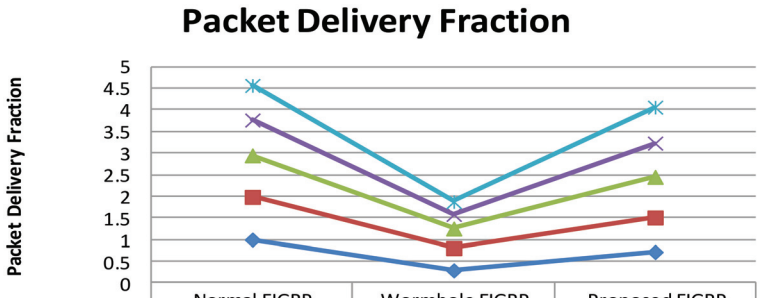
usually measured in data packets per second or bits per seconds. Throughput can be calculated by the amount of data transferred over a given period of time. So higher throughput means more number of data transferred from source to destination. Thus the throughput ratio will be increased for network.

In Figure 4, Average end to end delay includes all possible delay caused by buffering during route discovery latency. End to end delay refers to the time taken for a packet to be transmitted across a network from source to destination. End to end delay = Receiving time – Sent time. Compares normal EIGRP and wormhole EIGRP, the proposed EIGRP decreases the average end to end delay values.



	Normal EIGRP	Wormhole EIGRP	Proposed EIGRP
50 Nodes	99.25	109.254	89.632
40 Nodes	97.285	107.324	80.803
30 Nodes	79.37	87.193	78.943
20 Nodes	65.328	72.91	64.34
10 Nodes	97.414	107.868	97.368

Figure 4 Average end to end delay for 10,20,30,40 and 50 nodes.



	Normal EIGRP	Wormhole EIGRP	Proposed EIGRP
50 Nodes	0.8002	0.297	0.832
40 Nodes	0.818	0.327	0.782
30 Nodes	0.96	0.449	0.938
20 Nodes	0.987	0.512	0.793
10 Nodes	1	0.2939	0.718

Figure 5 Packet delivery fractions for 10, 20, 30, 40 and 50.

In Figure 5, after applying the proposed EIGRP, the results for packet delivery fraction improved. Here it can be easily identify the difference of wormhole EIGRP and proposed EIGRP. Packet delivery ratio defines the rate of data packets received at a destination according to the number of packets generated by the source node.

Packet Delivery Fraction = (No.of Packets received/No.of Packets sent)*100.

Here the performance of packet delivery ratio has higher than the other method.

4 Conclusions

In WSN, providing a safe communication is a difficult task. Hence, the proposed mechanism can be used to detect and prevent the wormhole attacks. All the mechanism done is calculated the Round Trip Time (RTT). Using EIGRP various constraints like average throughput, average end to end delay and packet delivery fraction is show that the improved result. In future this mechanism will be applied on MANET and ad-hoc network to detect and prevent the wormhole attack.

References

[1] Ronghui, H., Guoqing, M., Chunlei, W., and Lan, F. (2009). Detecting and locating wormhole attacks in wireless sensor networks using beacon nodes. *World Academy of Science, Engineering and Technology,* 55(31), 10–15.

[2] Chen, H., Lou, W., Sun, X., and Wang, Z. (2009). A secure localization approach against wormhole attacks using distance consistency. *EURASIP Journal on Wireless Communications and Networking,* 2010(1), 627039.

[3] Chen, H., Lou, W., and Wang, Z. (2009). Conflicting-set-based wormhole attack resistant localization in wireless sensor networks. In *International Conference on Ubiquitous Intelligence and Computing* (pp. 296–309). Springer, Berlin, Heidelberg.

[4] Lazos, L., and Poovendran, R. (2004). SeRLoc: Secure range-independent localization for wireless sensor networks. In *Proceedings of the 3rd ACM workshop on Wireless security* (pp. 21–30). ACM.

[5] García-Otero, M., and Población-Hernández, A. (2012). Detection of wormhole attacks in wireless sensor networks using range-free localization. In *2012 IEEE 17th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD),* (pp. 21–25). IEEE.

[6] Buttyán, L., Dóra, L., and Vajda, I. (2005). Statistical wormhole detection in sensor networks. In *European Workshop on Security in Ad-hoc and Sensor Networks* (pp. 128–141). Springer, Berlin, Heidelberg.

[7] Song, N., Qian, L., and Li, X. (2005). Wormhole attacks detection in wireless ad hoc networks: A statistical analysis approach. In *2005. Proceedings. 19th IEEE international Parallel and distributed processing symposium,* (pp. 8–pp). IEEE.

[8] Chiu, H. S., and Lui, K. S. (2006). DelPHI: wormhole detection mechanism for ad hoc wireless networks. In *2006 1st international symposium on Wireless pervasive computing,* (pp. 6–pp). IEEE.

[9] Sharif, M., Azeem, A., and Haider, M. R. W. (2012). A Novel Wormhole Detection Technique for Wireless Ad Hoc Networks. *International Journal of Advanced Networking and Applications,* 3(5), 1298.

[10] Jen, S. M., Laih, C. S., and Kuo, W. C. (2009). A hop-count analysis scheme for avoiding wormhole attacks in MANET. *Sensors,* 9(6), 5022–5039.

[11] Prakash, R. A., Jeyaseelan, W. S., and Jayasankar, T. (2018). Detection, Prevention and Mitigation of Wormhole Attack in Wireless Adhoc Network by Coordinator. *Appl. Math,* 12(1), 233–237.

[12] Kaur, P., Kaur, D., and Mahajan, R. (2017). Wormhole Attack Detection Technique in Mobile Ad Hoc Networks. *Wireless Personal Communications,* 97(2), 2939–2950.

[13] Jain, A., Sharma, S., and Buksh, B. Detection and Prevention of Wormhole Attack in Wireless Sensor Network. *International Journal of Application or Innovation in Engineering & Management,* pp. 138–142.

[14] Lai, G. H. (2016). Detection of wormhole attacks on IPv6 mobility-based wireless sensor network. *EURASIP Journal on Wireless Communications and Networking,* 2016(1), 274.

[15] Jain, R., Gupta, R., Rashmi, and Sandhya Katiyar. (2017). Detection and Prevention of Wormhole Attack In Adhoc Network Using Aodv Protocol. *International Journal of Computer Science and Mobile Computing,* pp. 241–248.

[16] Ji, S., Chen, T., and Zhong, S. (2015). Wormhole attack detection algorithms in wireless network coding systems. *IEEE transactions on mobile computing,* 14(3), 660–674.

[17] Patel, M. M., and Aggarwal, A. (2016). Detection of Hidden Wormhole Attack in Wireless Sensor Networks Using Neighbourhood and Connectivity Information, *International Journal on AdHoc Networking Systems,* pp. 1–10.

[18] Bendjima, M., and Feham, M. (2016). Wormhole attack detection in wireless sensor networks. In SAI Computing Conference (SAI), 2016 (pp. 1319–1326). IEEE.
[19] Nivedha, S., and Narayanan, S. S. (2015). Detection and prevention of wormhole attack in MANET using new fresh algorithm. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET),* 4(5), 2321–2326.
[20] Shrivastava, A., and Dubey, R. (2015). Wormhole attack in mobile ad-hoc network: a survey. *International Journal of Security and Its Applications*, 9(7), 293–298.
[21] Karthigadevi, K., Balamurali, S., and Venkatesulu, M. (2017). Improving Quality of Service, In Wireless Sensor Networks Using Neighbor Constraint Transmission Centric Distributed Sink Hole Detection And Network Simulator 2", *ARPN Journal of Engineering and Applied Sciences,* pp. 1197–1201.

Biographies

K. Karthigadevi received her Undergraduate degree in Computer Applications from Madurai Kamaraj University, Madurai, India, in 2004 and the post graduate degree in Computer Applications from Anna University, Chennai, India, in 2007. She worked as a faculty member at Arulmigu Kalasalingam College of Arts and Science from 2007 to 2009. Currently she is working as an Assistant Professor in the Department of Computer Applications at Kalasalingam Academy of Research and Education, Krishnankoil, Srivilliputtur, Tamilnadu, India from 2009 to till now. Her current research area is network security.

S. Balamurali is a Professor of Statistics and Director of Computer Applications at the Kalasalingam Academy of Research and Education. He received his undergraduate, postgraduate and doctoral degrees in Statistics from Bharathiar University, India. His research interests include applied statistics, data mining, network security and bioinformatics.

M. Venkatesulu received the postgraduate degree in Mathematics from Sri Venkateswara University, Tirupati, India, in 1975, and the Ph.D. degree in mathematics from Indian Institute of Technology, Kanpur, India, in 1979. He worked as a faculty member at Shri Sathya Sai University, Prashanthinilayam, India between 1983 and 2003. He also worked as a consultant for Satyam Computers, Hyderabad, India, for a short period. He was a Visiting Professor at University of Missouri, Kansas City, between August 2006 and May 2007. Currently he is working as a Senior Professor and Head of the Department of Information Technology at Kalasalingam University, Krishnankovil, Srivilliputtur, Tamil Nadu, and India. His area of interest includes differential equation, Image Processing, Cryptography, Bioinformatics, Big Data Analytics and Distributed Computing.