I. J. Computer Network and Information Security, **2018, 8, 17-26**
Published Online August 2018 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2018.08.02

Internet of Things for the Prevention of Black Hole Using Fingerprint Authentication and Genetic Algorithm Optimization

PoojaChandel
Dept. of Computer Science & Engineering, National Institute of Technical Teachers Training & Research, Chandigarh, India
E-mail: poojachandel5487@gmail.com

Rakesh Kumar
Dept. of Computer Science & Engineering, National Institute of Technical Teachers Training & Research, Chandigarh, India
E-mail: raakeshdhiman@gmail.com

Received: 08 January 2018; Accepted: 10 July 2018; Published: 08 August 2018

Abstract—The Internet is a communication network where two or more than two users communicate and exchange the data. Black hole attack is a security threat in which a malicious node drops some or all of the packets. The proposed framework implements a biometric authentication system into the communication network to verify the user and to save the user from any internal or external threat. The main objective is to integrate the biometric security with the communication network. The attack is supposed to be a Black hole which has been considered as a smart attack. Feature extraction of Fingerprint dataset will be done using minutiae extractor. This will extract ridge endings and ridge bifurcation from the thinned image. Genetic algorithm is usedto reduce the features to useful pool. If the user is authentic only then prevention mechanism against black hole is applied. Genetic Algorithm is used to find out black hole node based on the fitness function. Proposed model's performance is evaluated using various metrics like delay, throughput, energy consumption and packet delivery ratio.

Index Terms—Internet of Things, Black Hole, Genetic algorithm, Fingerprint authentication, Ad Hoc Network.

I. Introduction

IoT (Internet of Things) is a smart network which connects all the things to the internet for the purpose of exchanging information with agreed protocols. So, anyone can access anything, at any time and from anywhere.It is a rapidly spreading innovation that is changing the way in which human lives. In IoT network, things or objects are wirelessly connected with smart tiny sensors. As the Internet of Things keeps on growing from home indoor regulators to complex travel systems, propelled processing plants, interconnected financial systems, the security is progressively imperative [1]. IoT networks are unprotected against a wide range of malicious attacks. If security issues are not addressed then the confidential information may be leaked at any time. The usage of Fingerprint authentication over these business sectors and parts will include an abnormal state of security as well as keeping frameworks easy and simple to utilize.

Fingerprint authentication innovation gives an extraordinary level of security, making it the most effective approach to confirm one's personality besides DNA. It is very embeddable and suitable for use in numerous business sector areas, including social insurance, money related administrations, stadiums, car, government, and many more. As biometrics provide enhanced security in providing access to a particular device, it has become the desired authentication mechanism. As a result, it can be integrated into every facet of life. This technology is now being implemented and can be easily integrated into a network to provide high security in the network [2].

II. Blackhole Attack

In black hole attack, router instead of relaying packets to other nodes, drop some or all of the packets. In this routing protocol is used by a malicious node in order to advertise itself. It is hard to detect black hole attack as packets can also be dropped due to a network problem. If the router drops all the packets, then it is easy to discover the attack but if the router drops some of the packets over a particular period of time then it is difficult to discover black hole attack [3].

The faulty router broadcasts that it has the shortest way to the receiver's node than any other node. The faulty router does not check its routing table. Thus it sends a reply to the requests quickly before any other node. The requesting node gets a reply from the faulty node before

receiving a reply from an actual node. Thus forged route is created. After establishing the route, the faulty node will either forward the packet to unknown address or drop all the packets.

In Fig.1 node "A" sends RREQ packets to node "E" hence route discovery process is initiated. If node "B" is a malicious node then as it receives RREQ packet it sends the reply to node "A" before any other node. Thus node "A" considers it as the active route and initiates transferring the packets to the node "B". Node "A" will refuse all other replies from other actual nodes. Hence entire data packets will be lost [4].

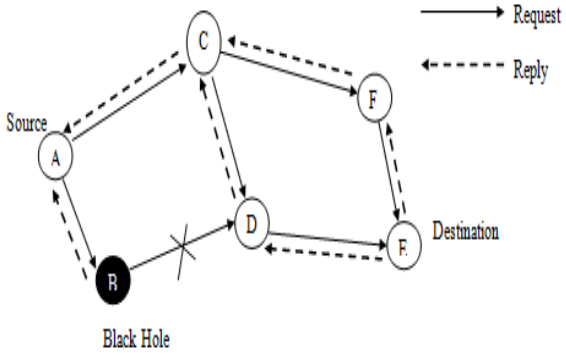

Fig.1. Black Hole Attack

III. FINGERPRINTAUTHENTICATION

Fingerprint matching is one of the oldest forms of the biometric technologies that is being used so widely. In the field of civilian, criminal investigation, government and commercial device applications like license card, passport and security device, the fingerprint technology is used. Fingerprints of humans are considered being unique and they can never be identical. Number of factors are there that lead to an interruption in fingerprint recognition such as small pressing spot, pressure, device noise, atmospheric factors and skin suppleness. Combination of patterns called ridges and valley develop the fingerprints. The single arched section is known as ridges andthe part between two adjoining ridges is known as valley and ridge termination is known as minutiae. For fingerprint matching mainly two features of minutiae are used i.e. ridge ending and ridge bifurcation [5].

A. Fingerprint Matching Techniques

i. Matching based on Correlation: For every alignment, two fingerprint images are taken and the relation between them takes place. For example a variety of displacements with rotations.

ii. Matching based on minutiae: Minutiae based matching as shown in Fig. 2 is being used in large part. Since the fingerprints are extracted and being saved in a 2-d plane as point sets. Minutiae-based matching basically looks for the position among the pattern and the outcome in the utmost figure of minutiae are set by the input minutiae.

iii. Matching based on ridges: For low-quality images, the extraction of minutiae is quite difficult in case of a fingerprint. The ridges of a fingerprint have a number of features that make it reliable to use than in case of minutiae. For the extraction of fingerprints, the pattern of ridges has the same approach [6].

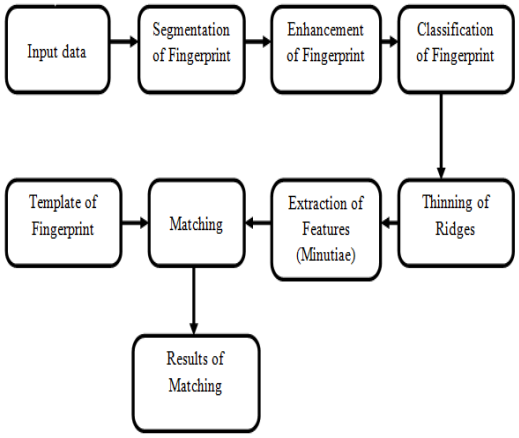

Fig.2. Fingerprint Identification System [6]

B. Approaches to Fingerprint Matching

i. Pattern Matching

It consists of four basic fingerprint patterns [7], as shown in Fig. 3:

a) Left loop: The ridge goes and came back from the finger's left surface.
b) Right loop: The ridges start and came back from the right surface.
c) Whorl: Ridges structures circularly in the region of a middle point.
d) Arch: The ridges go into one side, increase in the center form a curve and after that exit from the other side.

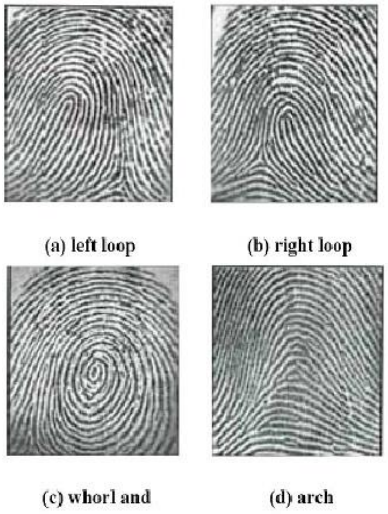

Fig.3. Types of Patterns [8]

ii. Minutiae Matching

Minutiae are considered as the fingerprint main features, with which the comparisons of one print with another can be drawn. It has:

a) Ridge ending- It is ridge's abrupt end.
b) Ridge bifurcation - Division of single ridge into two ridges.
c) Short ridge/Independent ridge - The ridge that travels a short distance and later gets terminated.
d) Island – A small ridge in a short ridge or ridge ending which is not linked to other ridges.
e) Ridge enclosure –The single ridge that firstly gets bifurcated and then reunites soon so as to continue as a single ridge.
f) Spur - Bifurcation within a small ridge branching off a larger ridge.
g) Crossover or bridge –The small ridge that runs between two parallel ridges [8].
h) Delta – A Y-shape formed ridge meeting.
i) Core – A U-turn in the ridge pattern.

IV. Genetic Algorithm

Genetic algorithm (GA) is inspired by the biological evolutions which are effective for searching domain-independent methods. These methods can help the user for solving the problems in a varied number of application domains. The idea of GA, given by Holland has two folds:

i. To abstract and define the nature's adaptive process.
ii. To design the artificial system software for retaining the nature's important mechanisms.

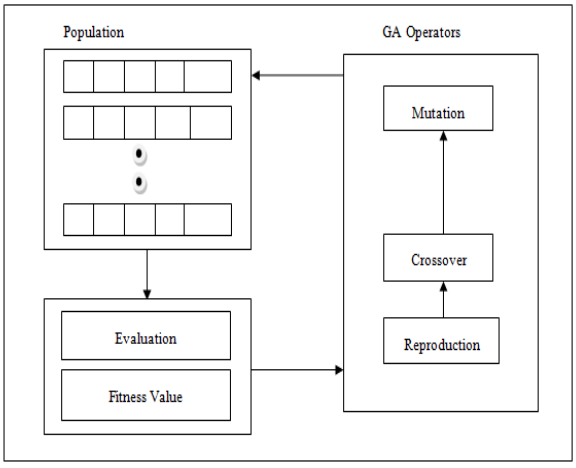

Fig.4. Genetic Algorithm Evolution Flow

As per Artificial Intelligence research, the method proposed by Holland gives a better mechanism for learning [9].

GA is said to be population dependent searching method for maintaining the solutions while searching. A string having fixed bit-length mainly shows the potential outcome. For evaluating that outcome, GA requires payoff/reward/objectives for assigning scalar payoff for the exact outcome. GA starts searching when the representation scheme and evaluation scheme is decided.

Fig. 4 explains the flow of the GA evolution.Firstly, GA generates some number, known as the population size from the first generation of strings. Next, for evaluating the solution for the first generation, payoff function is used. A good solution has maximum payoffs.

Later, generic operations are appointed for creating the next generation on the basis of these evaluations. The layout of evaluation and creation is performed till the optimal outcome is achieved or when the time assigned to the computation ends.

A. Components of Genetic Algorithm

Five components of the Genetic algorithm are as follows:

a) Solutions for the chromosomal representation to the problem.
b) Functions used for the evaluation of the problem for the solution.
c) The population used for initialized solutions.
d) The genetic operators that develop the population.
e) The metrics for specifying the probabilities through which the genetic operators can be applied [10].

i. Representation

Representation is problem dependent. It is called as genetic algorithm key because GA manipulates the representation of the coding for the problem. Therefore, the use of character sets and coding schemes takes place. In GA, the individuals are shown as the fixed length strings that show the fixed length strings for expressing fixed binary strings, which shows the schema as alphabet pattern {0,1,*} and gives binary strings set in the searchspace. Thus, each string consists of 2^L schemata, and L is the length of a binary string.

ii. Evaluation Function

The evaluation function is also problem dependent. GA is said to be a search technique which is dependent on the feedback received from the study of the solutions. The best optimal solution for GA exploration is known as the Evaluation function for each population of GA. The idea for evaluation and fitness are occasionally used interchangeably. The evolution function provides a measure of user's performance, and the fitness function gives a calculation for individual's performance. The assessment of the individual is independent of another individual and the fitness of an individual mostly dependent on other individuals [11].

iii. Initial Population

To choose a suitable population size for GA is essential but complex tasks for all Genetic users. If the population is small then the GA converges quickly for finding the optimal solution but if the population size is very large then computation cost may get increased.

iv. Operators

According to the mechanism point of view, GA is an iterative process where iteration consists of two basic steps- evaluation and generation. In an evaluation, the information domain is used for evaluating the quality of the individual. In selection, fitness is utilized for guiding the reproduction of novel candidates for the subsequent iterations.

v. Fitness Function

Fitness function maps a user to a unique number for indicating the number of offsprings that a user is expecting to strain. The high fitness users basically have more emphasis on the following generations because these are selecting more frequently. When the recombination phase started, the crossover and mutation perform integrated. The crossover re-constructs selected individuals for creating two novel offspring. Mutation is for re-introducing the involuntary loss of genetic value. Many researchers have focused on selection, mutation and crossover. The selection depends on fitness, mutation and crossover are the investigating resources. The genetic combines the utilization of past results with the novel fields of the search space. GA depends very much on exploration and exploitation [12].

B. Operators of Genetic Algorithm

i. Selection

To get better individual, selection operator has an important role. It has been noted by some authors that this phase can be divided into selection and sampling algorithm. Selection algorithm assigns a real number to each individual, called as a target sampling rate, for indicating the expected offspring number that use to reproduce at the time. Sampling algorithm actually reproduces, depending on the target sampling rate, to produce the population. There is a difference between the actual and expected probability sample of individuals. That difference is called as bias.

There are basically two types of selection algorithm, namely the explicit and implicit fitness remapping. Explicit fitness remapping remaps the fitness to the novel scale. It is later used by the sampling algorithm. Fitness ranking and proportional rank come under this field. Implicit fitness remapping fills the matching pools instead of passing via the intermediate remapping step.

ii. Crossover

The crossover is known as mainly the important re-combination operator. One-point crossover is a commonly used method that selects two individuals from the population that exchanges the representation portions. Assume one point crossover as an example. Individuals are shown as binary strings.

In a single-point crossover, a point is called as Crossover point that is chosen randomly with the segments to the right of the points chosen randomly and the exchanging of the segments to the right is taken place [13]. Let's take an example, that has x1=101010 and x2=010100 and receives the crossover points among 4 and 5 bits. The example is shown in the Fig. 5.

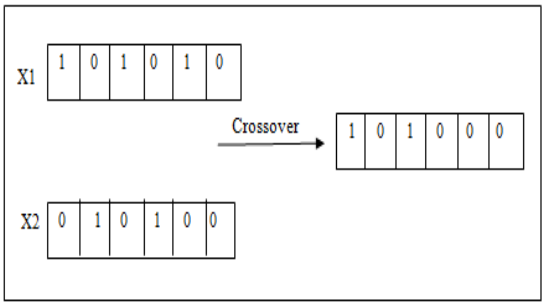

Fig.5. Crossover

The crossover has two matching search abilities. Primarily, it has new points for testing the hyperplanes that are already shown in the population. Secondly, it has representatives of novel hyperplanes in the population.

iii. Mutation

When the users are shown as the bit a string, then the mutation consists of reversing a bit which is randomly chosen. Lets take an example when the individuals are taken as binary strings. When the bit is selected for a mutation then it would be flipped for matching with the value of an original bit in the bit complement. If X1=101010 and the mutation bits are 4, then the child came out to be X2=101110. The example is shown in the Fig. 6.

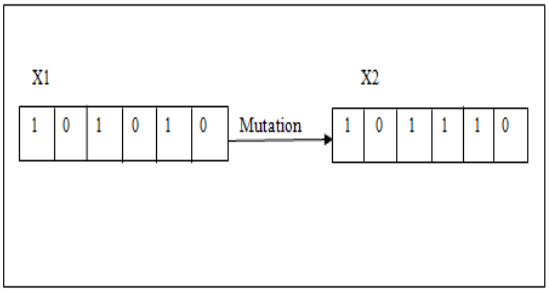

Fig.6. Mutation

If the number has bits group in the string, minute amendments to the values could be followed by such mutations. It prevents the GA from the refinement of the solutions after finding the better solutions in its neighborhood.

V. Related Work

Mouad.M.H.Ali et al. [14], presented a fingerprint recognition system that is divided into four stages. (i) Acquisition (ii) Pre-processing (iii) Feature extraction (iv) Matching stage. The first stage collects fingerprint image. The second stage performs image enhancement, thinning etc. The third stage by using minutiae extractor method extracts the features from the thinning image. The fourth stage matches two minutiae points by using matcher method. For testing, images are taken from FVC2000 and

FVC2002 databases. Images from FVC2002 database shows better result. For evaluation, the parameters that are used here are False Acceptance Rate and False Rejection Rate. The result of FAR is 0.0154, FRR is 0.0137, and the accuracy is 98.55%.

Bikramjeet Singh et al. [15], described cooperative and single black hole attack in which a malicious nodespoofing the source node. Researchers around the world present a variety of detection technologies and solutions to detect this type of security attacks. The author proposed a hybrid technology to mitigate the effects of black hole attacks. NS-2 simulator is used for simulation. Parameters like throughput, delay and packet transmission rates are used.

Ashish et al. [16], proposed a new protocol named as Secure AODV for preventing the effect of black hole attack on the network. It is based on first route reply caching mechanism. In this protocol, to mitigate the black hole attack, the first RREP that is reaching the source node is ignored. The results are measured using various parameters like packet delivery ratio, delay and throughput that show a considerable improvement over existing protocol.

M. Rajesh Babu et al. [17], proposed an alleviation procedure to detect the nodes that are behaving abnormally. Sensitive guard procedures, hole detection algorithms and timely mandate procedures are used to detect hostile nodes. The proposed procedure is cost-effective and ensures the guaranteed QoS by assuring resource availability. From the results, authors hadconcluded that proposed algorithm is better than other solutions for the detection of black hole attack.

Arshdeep et al. [18], implemented genetic algorithm with Black hole attack. In this paper, dynamic source routing protocol is used to prevent a system from attack. For simulation, a hypothetical network was constructed and then monitored for a number of parameters.

Chandeep Singh et al. [19], proposed an adaptive approach based on genetic optimization to determine Blackhole attack in AODV (Adhoc on demand distance vector protocol). The Genetic algorithm is used to increase the performance, availability and efficiency of the network. They had analyzed the performance of GAin AODV protocol during black hole attack and concluded that AODV–GA is better than only AODV.

Rakesh Ranjan et al. [20], reviewed black hole attack. Black Hole attack affects reactive routing protocol that causes a serious loss of data which leads to a security threat. As one of many protocols AODV (Ad hoc On-demand Distance Vector) is usually an easy victim of such attacks. In this type of attack, the node broadcasts that it has the shortest path to the destination and making it easier to access all of the data transmitted. Such nodes are called malicious nodes.

Purneet Kaur et al. [21], proposed a technique in which Genetic algorithm and Neural Network are combined together. For extraction of minutiae GA is used and for the recognition of finger print neural network is used. For processing low and high-resolution images histogram equalization process is used. Thinning of lines is done on MATLAB using morphological image processing. The Genetic algorithm is used to find out discontinuous segments. At last, for matching processed image is fed to the trained system. Experimental results show that combination ofgenetic algorithm and neural network provides better and efficient technique for finger print matching.

VI. Methodology

A network model is considered which consists of N number of nodes which exchange data. The main objective of this research work is to integrate the biometric security with the communication network. Here we will describe the black hole attack scenario in the network. To gain access to the system, the user must be identified first and then further checking is done to verify the identity. This work will utilizeminutiae feature extraction, feature reduction and failure node detection using a genetic algorithm. Simulation of the proposed protocol is done in MATLAB version 2010a.

The entire methodology of proposed work is given below:

Step 1: The first step is to upload the fingerprint images.

Step 2: Apply pre-processing on the uploaded fingerprint image.

Step 3: Feature extraction of Fingerprint dataset will be done using minutiae extractor. This will extract ridge endings and ridge bifurcation from the thinned image.

Step 4: Then obtained number of features must be reduced to a useful pool and it will be done by the genetic algorithm using fitness function.

Step 5: For the training phase store the trained images in database and in case of testing upload the image and apply pre-processing, feature extraction and feature optimization method.

Step 6: Now check if the user is authenticated or not by checking whether the Fingerprints are matched or not.

Step 7: If the user is authentic then initialize the network in which area must be specified to show the attack detection and prevention. By default, the selected area is 1000 * 1000 having N number of nodes.

Step 8: Then transmission of data starts taking place from source to destination using shortest path routing algorithm.

Step 9: After this occurrence of the black hole attack in the network will be shown. If the user is authentic then apply prevention mechanism using genetic algorithm. If the user is not

authentic then prevention mechanism is not applied.

Step 10: At last evaluate the model's performance by metrics like throughput, packet delivery ratio, energy consumption and delay. A system must have high throughput and low delay to have a good rate of performance.

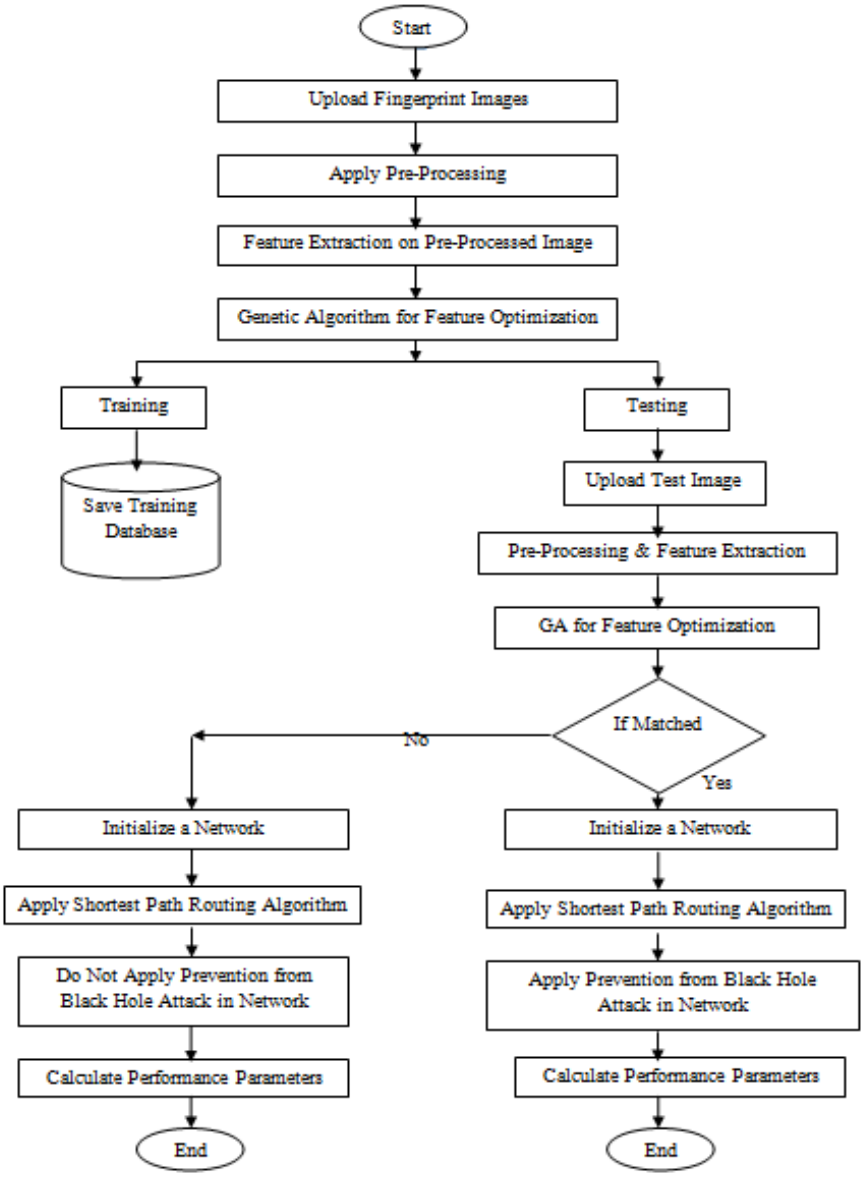

Fig.7. Flow Chart of Proposed Methodology

VII. EXPERIMENTALRESULTS

Simulation of the proposed model is done in MATLAB version 2010a. A dataset has been prepared for the fingerprint in testing panel. The experiments are tested on fingerprint database FVC2002. The area in the proposed network consists of 1000× 1000 having 50 numbers of nodes. The network is run for five times that means five iterations have been applied to run the network so that best results are obtained.

A. Performance Parameters of the Proposed Work

The simulation is performed to evaluate various performance metrics like throughput, packet delivery ratio, energy consumption and delay.

Table 1. ParameterValues With and Without Prevention

Network parameter	Without prevention	With prevention
Throughput	101	150
Packet delivery ratio (%)	1.32	1.84
Energy Consumption (J)	0.86	0.54
Delay (msec)	9.84	7.1

These metrics are evaluated by comparing their

performances when prevention is applied and when there is no prevention mechanism. The average value obtained for each parameter is shown in Table 1.

i. Throughput

In Fig. 8, the blue line indicates the values obtained for the proposed network when no security has been applied whereas; red line indicates the value of throughput obtained with the security algorithm. As it is clear from the figure when no security has applied the value of throughput is less.

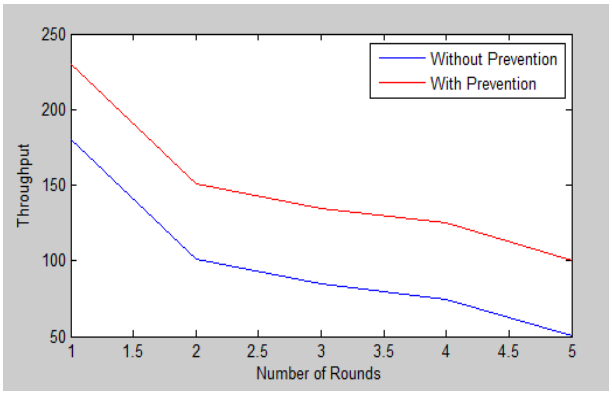

Fig.8. Throughput With and Without Prevention

When prevention techniques are applied to the network the value of throughput is high. The value obtained for each iteration is shown in Table 2.

Table 2. ThroughputValues With and Without Prevention

Number of rounds	Without prevention Throughput	With prevention Throughput
1	180	230
2	100	150
3	90	140
4	85	130
5	50	100

ii. Packet Delivery Ratio

In the Fig. 9, the blue line indicates the values obtained for the proposed network when no security has been applied whereas; red line indicates the value of throughput obtained with the security algorithm.

As it is clear from the figure that when no security is applied the value of PDR is less and when security is applied the value of PDR is high. More PDR means a large number of packets is received at the receiver.The value obtained for each iteration is shown in Table 3. From the table, we are concluding that the average value of PDR without prevention is 1.32, whereas with prevention algorithm it gets increased and becomes 1.84.

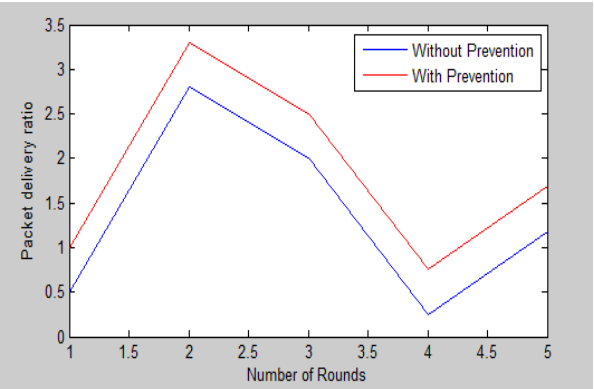

Fig.9. Packet Delivery Ratio With and Without Prevention

Table 3. Packet Delivery RatioValues With and Without Prevention

Number of rounds	Without prevention PDR (%)	With prevention PDR (%)
1	0.5	1.0
2	2.7	3.3
3	2.0	2.5
4	0.2	0.7
5	1.2	1.7

iii. Energy Consumption

When transmitting signal from one node to another node, each node will consume some energy. Ideal node consumes less energy as compared to the busy node. Thus, it is necessary to determine the route which consumes less power for transmitting the data successfully. Hence a routing protocol that considered the residual energy will perform better than the protocol that does not.

From Fig. 10, it is clear that energy consumption is high when no algorithm has been applied. When optimization algorithm like GA has been applied energy consumed by node get decreased.

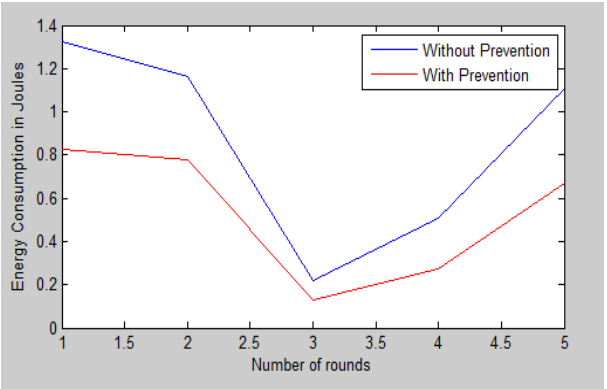

Fig.10. Energy Consumption With and Without Prevention

The value obtained for each iteration is shown in Table 4. From the table we are concluding that the average value obtained for the network without prevention is 0.86

whereas with optimization or when prevention is applied energy consumption get reduced and becomes 0.54.

Table 4. Energy Consumption Values With and Without Prevention

Number of rounds	Without prevention Energy consumption (J)	With prevention Energy consumption (J)
1	1.32	0.82
2	1.18	0.79
3	0.22	0.12
4	0.50	0.30
5	1.10	0.67

iv. Delay

This metric is calculated by subtracting time at which the first packet was transmitted by the source from the time at which first data packet arrived at the destination.

It is clear from the Fig. 11 that delay obtained without prevention techniques is more than with prevention techniques.

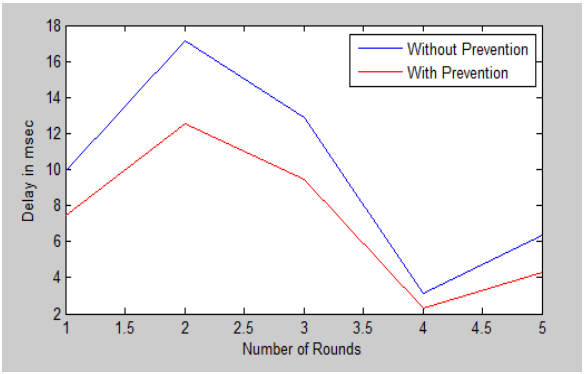

Fig.11. Delay With and Without Prevention

The value obtained for each iteration is shown in table 6.4. From the table, we are concluding that the average value obtained for delay without prevention is 9.84 whereas with optimization or when prevention is applied delay get reduced and become 7.1.

Table 5. Delay Values With and Without Prevention

Number of rounds	Without prevention Delay in msec	With prevention Delay in msec
1	10	7.5
2	17	12.4
3	13	9.2
4	3	2.2
5	6.2	4.2

B. Comparison Against Other Method

The conclusion of simulation has been shown in the following graphs. Throughput, packet delivery ratio and delay metrics are evaluated by comparing their values with the proposed mechanism and existing mechanism.

i. Throughput

Let us first analyze the throughput of the proposed method in comparison with an existing method.In the table below the comparison between existing work and proposed work is shown. It is concluded that the throughput of our work is better than the existing work.

Table 6. Comparison of Throughput Values With Existing and Proposed Work.

Number of rounds	Existing method Throughput	Proposed method Throughput
1	60	230
2	30.4	150
3	30.4	140
4	30	130
5	30	100

At a number of rounds corresponding to value 1, the existing method has shown a value of 60, whereas for proposed method a value of 230 has been observed. A similar trend has been observed for the number of rounds corresponding to 2, 3, 4 and 5 as evident from Fig. 12. Fig. 12 shows that proposed method performs better as the values of throughput are comparatively high to the values of an existing method.

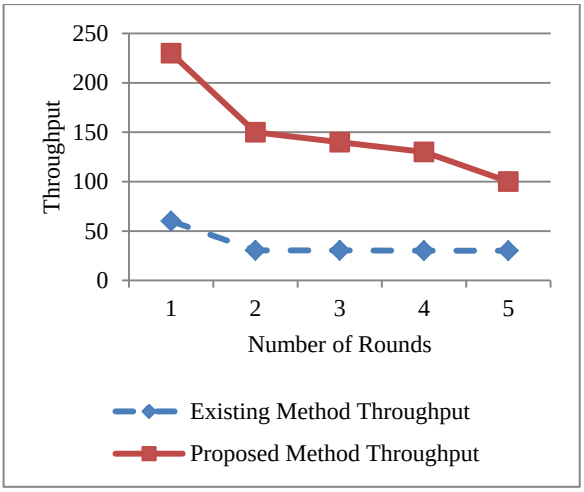

Fig.12. Existing and Proposed Method Throughput

ii. Packet Delivery Ratio

In Table 7, the comparison between existing work and proposed work is shown. It is concluded that the packet delivery ratio of our work is better, as existing work has lost more packets.

For example, at the number of rounds corresponding to value 1, the existing method has shown a value of 38, whereas for proposed method a value of 26 has been

observed. Here the value has decreased for the proposed method but after that, there is an increase in the values.

At the number of rounds corresponding to value 2, the existing method has shown a value of 22, whereas for proposed method a value of 40 has been observed.

Table 7. Comparison of PDR Values with Existing and Proposed Work

Number of rounds	Existing method packet delivery ratio (%)	Proposed method packet delivery ratio (%)
1	38	26
2	22	40
3	21	21
4	20	37
5	19	28

A similar trend has been observed for the number of rounds corresponding to 3, 4 and 5 as evident from Fig. 13 and values elaborated in table 7. The below graph shows that proposed method performs better ascompared to the existing method.

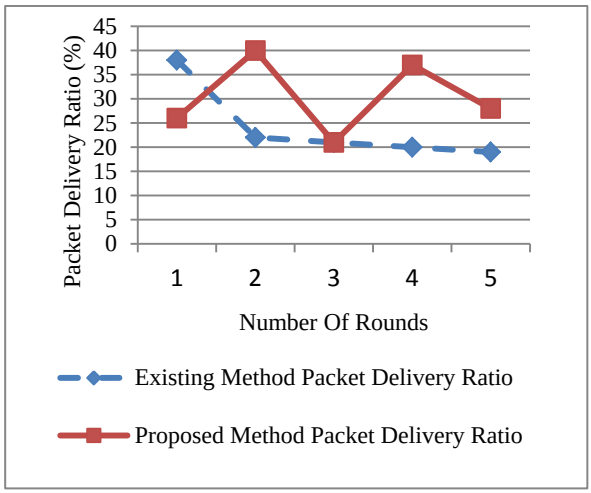

Fig.13. Existing and Proposed Method PDR

iii. Delay

In table 8, the comparison between existing work and proposed work for delay obtained in the network is shown. It is concluded that the delay of our work is less than the existing work.

Table 8. Comparison of Delay Values with Existing and Proposed Work

Number of rounds	Existing method delay in msec	Proposed method delay in msec
1	8.5	7.5
2	8.5	12.4
3	9.8	9.2
4	12.2	2.2
5	10	4.2

For example, at the number of rounds corresponding to value 1, the existing method has shown a value of 8.5, whereas for proposed method a value of 7.5 has been observed.At the number of rounds corresponding to value 2, the value of delay has increased for the proposed method but after that, there is a decrease in the delay as shown in Fig.14.

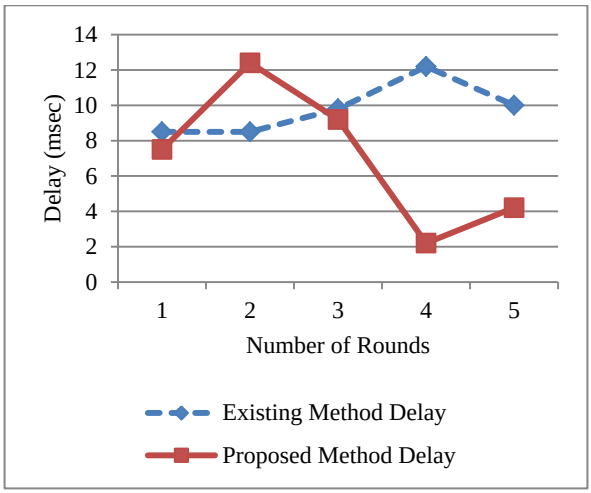

Fig.14. Existing and Proposed Method Delay

VIII. Conclusion & Future Scope

From the experimental outcomes, it can be determined that the proposed methodology gives efficient results. The proposed work is used to authenticate the black hole attack in the IoT by using a unique fingerprint. A dataset has been prepared for the fingerprint in the testing panel. The experiments are tested on fingerprint database FVC2002. In the proposed work performance parameters like throughput, delay, energy consumption and packet delivery ratio have been measured and concluded that when prevention techniques havebeen applied the value of throughput and PDR get increased whereas the value of energy consumption and delay get decreased. Results show that this approach performs better than other similar approaches in almost all cases.

In future work, multimodal biometrics can be used for the security purpose in which more features can be recognized and thus the performance of the network gets increased. For optimization and classification hybrid technique can be used in which more than one optimization algorithm can be applied. Fuzzy logic can be used for classification.

References

[1] Zeinab Kamal Aldein Mohammed, Elmustafa Sayed Ali Ahmed, “Internet of things applications, challenges and related future technologies”, World Scientific News, pp. 126-148, 2017.

[2] Suchitra, Vandana, “Internet of things and security issues”, International Journal of Computer Science and Mobile Computing, Vol. 5, Issue. 1, pp. 133-139, Jan. 2016.

[3] C. K. Nagpal, Chirag Kumar, Bharat Bhushan, Shailender

Gupta, "A study of black hole attack on MANET performance", IJMECS, vol.4, no.8, pp.47-53, 2012.
[4] Kumar Roshan,Vimal Bibhu,"Preventive aspect of black hole attack in mobile AD HOC network", IJCNIS, vol.4, no.6, pp.49-55, 2012.
[5] Aditi Roy, Nasir Memon, Arun Ross, "Masterprint: exploring the vulnerability of partial fingerprint-based authentication systems", IEEE Transactions on Information Forensics and Security, Vol. 12, Issue. 9, pp. 2013-2025, Sept. 2017.
[6] Manisha Redhu and Balkishan, "Fingerprint recognition using minutiae extractar", International Journal of Engineering Research and Applications (IJERA), Vol. 3, Issue 4, pp. 2488-2497, August 2013.
[7] Samayita Bhattacharya, Kalyani Mali, "Fingerprint recognition by classification using neural network and matching using minutiae (fingerprint recognition by NNMM Method)", International Journal of Emerging Research in Management &Technology, Vol. 3, Issue 8, pp. 1-10, Aug. 2014.
[8] Ruud M. Bolle, Nalini K. Ratha and Sharath Pankanti, "Fingerprint minutiae: a constructive definition", Springer International Workshop on Biometric Authentication, pp. 58-66, 2002.
[9] Richa Garg, Saurabh mittal, "Optimization by genetic algorithm", International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4, pp. 587-589, April 2014.
[10] Andras Rozsa, Albert E. Glock, Jr, Terrance E. Boult, "Genetic algorithm attack on minutiae-based fingerprint authentication and protected template fingerprint systems", IEEE Conference on Computer Vision and Pattern Recognition Workshops, pp. 100-108, 2015.
[11] K. F. Man, K. S. Tang, and S. Kwong, "Genetic algorithms: concepts and applications", IEEE Transactions on Industrial Electronics, Vol. 43, No. 5, pp. 519-534, Oct. 1996.
[12] Pushpendra Kumar Yadav, Dr. N. L. Prajapati, "An overview of genetic algorithm and modeling", International Journal of Scientific and Research Publications, Vol. 2, Issue 9, pp. 1-4, Sept. 2012.
[13] Meenakshi Moza, Suresh Kumar, "Improving the performance of routing protocol using genetic algorithm", International Journal of Computer Network and Information Security(IJCNIS), Vol.8, No.7, pp.10- 16, 2016.DOI: 10.5815/ijcnis.2016.07.02.
[14] Mouad. M. H. Ali, Vivek H. Mahale, PravinYannawar and A.T. Gaikwad, "Fingerprint recognition for person identification and verification based on minutiae matching", 6th IEEE International Conference on Advanced Computing (IACC), pp. 332-339, 2016.
[15] Bikramjeet Singh, Dasari Srikanth, and C.R. Suthikshn Kumar, "Mitigating Effects of Black Hole Attack in Mobile Ad-Hoc Networks: Military Perspective", 2nd IEEE International Conference on Engineering and Technology (ICETECH), March 2016.
[16] Ashish Kumar Jain and VrindaTokekar, " Mitigating the effects of black hole attacks on AODV routing protocol in mobile ad hoc networks", IEEE International Conference on Pervasive Computing(ICPC), pp.1-6, 2015.
[17] M. Rajesh Babu, S. Moses Dian, Siva Chelladurai and Mathiyalagan Palaniappan, "Proactive Alleviation Procedure to Handle Black Hole Attack and ItsVersion", The Scientific World Journal, Vol. 2015, pp. 1-12, 2015.
[18] Arshdeep Kaur, Mandeep Kaur, "Prevention of black hole attack in manet using genetic algorithm", International Journal of Advance Research in Science and Engineering, Vol. 4, pp. 153-163, May 2015.
[19] Chandeep Singh, Vishal Walia, Rahul Malhotra, "Genetic Optimization based Adaptive Approach for the Determination of Black Hole Attack in AODV Protocol", 2nd International Conference on Science, Technology and Management, pp. 2742-2753, 2015.
[20] Rakesh Ranjan, Nirnemesh Kumar Singh, "Security Issues of Black Hole Attacks in MANET ", IEEE International Conference on Computing, Communication and Automation (ICCCA), pp. 452-457, 2015.
[21] Purneet Kaur, Jaspreet Kaur, "Finger print Recognition Using Genetic Algorithm and Neural Network", International Journal of Computational Engineering Research, Vol. 3, pp. 41-46, 2013.

Authors' Profiles

PoojaChandel is pursuing M.Tech. (Computer Science) at National Institute of Technical Teachers Training and Research, Chandigarh, India. She received B.Tech. in Computer Science and Engineering from Green Hills Engineering College, Solan, India. Her research interest includes Ad hoc Networks, Internet of Things and Network Security.

Rakesh Kumar is an Assistant Professor at the Department of Computer Science and Engineering, National Institute of Technical Teachers Training and Research, Chandigarh, India. He received his Ph.D. (Computer Engineering) from NIT Kurukshetra, M.Tech. (IT) from GGS IndraprasthaUniversity, Delhi, B.Tech. in Computer Science and Engineering from Punjab Technical University, Jalandhar. His research interest includes Cloud Computing and Adhoc Networks.

How to cite this paper: PoojaChandel, Rakesh Kumar,"Internet of Things for the Prevention of Black Hole Using Fingerprint Authentication and Genetic Algorithm Optimization", International Journal of Computer Network and Information Security(IJCNIS), Vol.10, No.8, pp.17-26, 2018.DOI: 10.5815/ijcnis.2018.08.02