A Hybrid Method for Blocking Malicious Nodes and Optimal Path Identication In Mobile Adhoc Networks

Diana P Varghese, Vinodh P Vijayan

Abstract— Intermediary nodes play a great role in networking for smooth communication because they provide connectivity and work behind the scenes to ensure that data flows across the network. These nodes connect end devices to the network and can connect multiple individual networks to form an internetwork. This paper presents a hybrid mechanism which consist of Elliptical Curve Cryptography and Genetic algorithm. This method helps to improve the correctness and quality of the network. The new method aimed at improving the accuracy of misbehavior detection by identifying optimal path. Intermediary nodes in the network is analysed initially and identified the defected nodes using Elliptical curve cryptography. In the second phase optimal path for packet transmission is identified using genetic algorithm. The experiment is done using Network Simulator 2 (ns2). It indicates that this mechanism provide considerable improvements in the blocking of malicious node and optimal path identification thereby improving the performance of MANET.

Index Terms— Elliptical curve cryptography (ECC), Elliptical curve Diffie-Hellman Algorithm (ECDH), Elliptical curve Digital Signature (ECDS), Genetic Algorithm (GA), fitness function, Mobile adhoc networks (MANETs).

1 Introduction

MANET is an emerging technology which enables users to communicate anywhere at anytime. It is a type of ad hoc network that change locations and configure itself. Each device in a MANET is free to move independently in any direction and will therefore change its links to other devices frequently. It is a self configuring self organized in which nodes acts as both sender and receiver. It doesnot need any centralized administrator for communicating. Nodes can forward the packet to source and destination within their transmission range. Minimal configuration and quick deployment makes manet suitable for emergency situations such as military exercises, search and rescue, disaster relief operations, data monitoring. It can also be used in civilian environments like sport stadiums, meeting rooms, business.

End to end data transfer, security, link access control are some of the challenges in this area. Fig.1 shows the MANET architecture which does not have any centralized administration. The routers are free to move randomly and organize themselves in random. Thus they can change the topology randomly and unpredictably.

Security [1] and optimal path identification is always a challenging factor in MANET. The current mobile adhoc is prone to many security issues such as grey hole attacks , lack of cooperation, misrouting , information disclosure, malicious activities and so on. It is also failed to find out an trusted path for transmission.

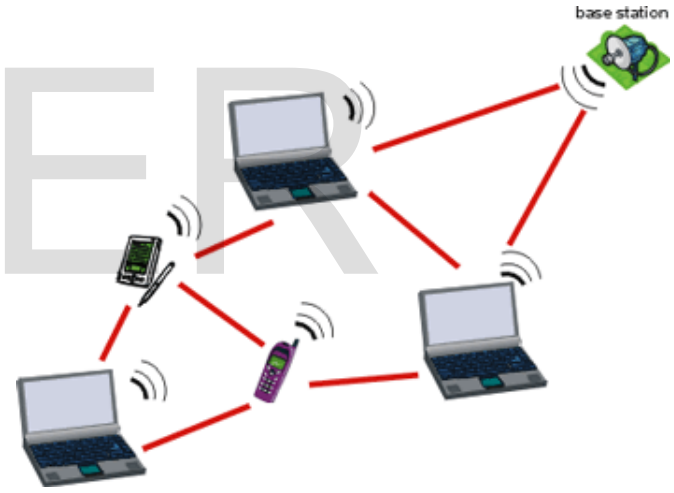


Fig.1 Mobile Adhoc Network

2 Existing Method

Researches provide different solutions for providing security in MANET. A lot of solution has been proposed. None of them have made a tradeoff between blocking malicious and optimal path identification. Elhadi and Tarek proposed EAACK [2] an acknowledgement based intrusion detection mechanisms. It consist of three phases such as ACK, Secure ACK(S-ACK), and misbehaviour report authentication (MRA). However, the network overhead will be high. Jian-Ming propose a method called cooperative bait detection scheme [3] to prevent malicious node in MANET. It integrates the proactive and architectures and randomly cooperates with

- *Diana P Varghese is currently pursuing masters degree program in computer science and engineering in Mangalam College Of Engineering, MG University, Kottayam ,Kerala, India E-mail: dianapvarghese@gmail.com*
- *Vinodh P Vijayan is currently working as associate professor in Mangalam College Of Engineering ,MG University, Kottayam ,Kerala, India , E-mail: vinodh.pvijayan@gmail.com*

a stochastic adjacent node. Marti et al [4] suggest a solution to improve throughput in adhoc network. But it cannot find out malicious activities in the presence of receiver collision.

An acknowledgement based Adaptive ACKnowledgement (AACK) [5] scheme was proposed to overcome watchdog weakness such as collisions and limited transmission power and also to improve the problems with TWOACK scheme [6]. This scheme is to identify the exact misbehaving node on the misbehaving links.

Saurabh Gupt [7] proposed a protocol BAAP for detecting malicious activities in the path using legitimacy table maintained by each node in the network. Adhoc on demand multipath distance vector (AOMDV) is used to form link disjoint multipath during path discovery. When intermediary nodes reply to source node, it eventually identifies only one path to destination node. Here each node is supposed to maintain a legitimacy table which contains the most legitimate node to source node and next hop to destination.

Nei kato [8] proposed dynamic anomaly detection by using dynamic learning process. It involves the method to calculate the projection distance and compare it to baseline profile using PCA. ECC [9] is used for identifying the malicious node with smaller keys. But it is failed to find the optimal path.

Goto [12] propose a method known as ECC encryption and decryption which provides suffiecient strength against crypto analysis whose performance are compared with standard algorithms like RSA.

3 Malicious Node Detection Using ECC And Optimal Path Identification Using GA

The proposed work is a hybrid mechanism which focus on identifying the misbehaving node and find out optimal path. So in initial phase the malicious node is detected and blocked which is followed by optimal path identification. So ECC algorithm is implemented at the initial phase. In the second part optimal path is discovered using genetic algorithm.

3.1 System Model

The fig.2 shows the hybrid method in MANET. Fig.3 (a),(b) describes the malicious node blocking and optimal path identification. It consisting of two phases blocking of malicious node using ECC algorithm(section 3.2) . In second phase application of GA is applied (section 3.4). The detailed operations are shown in fig.3.

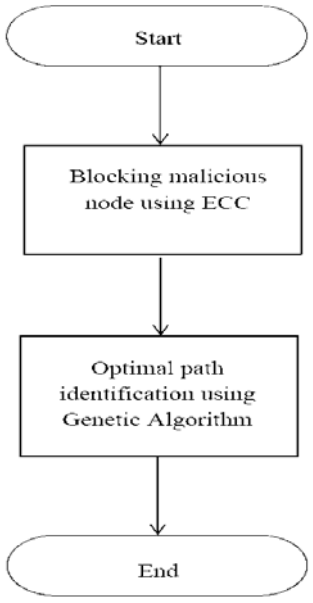
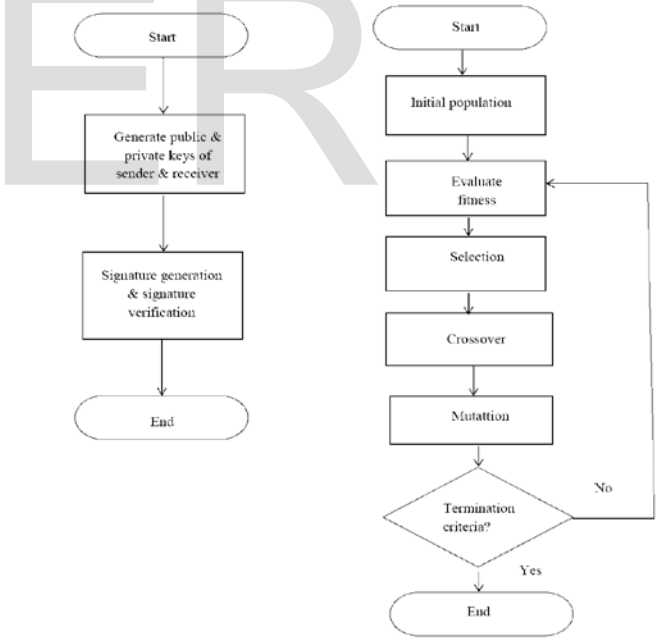


Fig.2 Blocking of malicious node and optimal path identification



(a) (b)

Fig.3 The procedure in the malicious node detection & Optimal path identification

3.2 The Elliptical Curve Cryptography Algorithm

Cryptography is generally used to provide security in MANET. The ECC is a next generation public key cryptography based on algebraic structure of elliptical curve over a finite

fields. Because of its smaller key size, faster computation, lower power consumption, aswell as memory and bandwidth savings it is more secured than other traditional cryptographic algorithms. A finite field usually consist s of the points satisfying equation

$$y^2 = x^3 + ax + b \quad (1)$$

where a and b are the constant values from the finite field. The curve is set of pairs of values (x,y) which match the equation. In ECC, a public and private keys are used for encryption/signature verification and decryption/signature generation [9] respectively. It defines a set of algorithms such as Elliptic Curve Diffie-Hellman for key exchange aand Elliptical Curve Digital Signature for signature generation.

The fig.2 shows the hybrid method in MANET. Fig.3 (a),(b) describes the malicious node blocking and optimal path identification (section) .

Elliptic Curve Diffie-Hellman Key Exchange Algorithm

It is an anonymous key exchange algorithm which consist of two parties having an elliptic curve public-private key pair to establish a shared secret key over a malicious channel. Fig.4 shoes ECCDH mechanism.

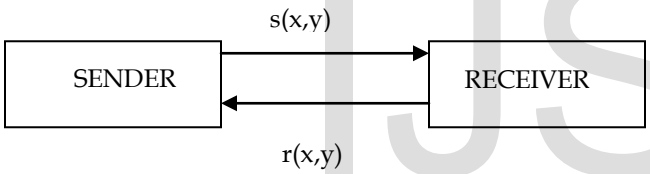


Fig.4 ECC Diffie-Hellman

Step 1 Select a random integer f from [1, n-1].
Step 2 Calculate Q = dG
2.2 Sender
2.2.1 Private key = d
2.2.2 Public key = Q

Elliptic Curve Digital Signature

Steps for signature generation is given below.

Step 1 Select a random integer i from [1,n-1]
Step 2 Compute iG = (x1,y1) and r = x1mod n.
If r = 0 go to step 1.
Step 3 Compute i^{-1} mod n.
Step 3 Compute H(m) , where H is a hash function.
Convert the result to an integer e
and m is the message.
Step 4 Compute j = i^{-1}(e+dr) mod n. If j = 0 go to step 1
Step 6 Sender's signature for the message m is (i,j)

Steps for signature verification

Step 1 Verify i and j are in the interval [1 , n-1]
Step 2 Compute e = H(m) , where H is a hash function and m is the message.
Step 3 Compute w = j^{-1} mod n
Step 4 Compute u_1=ew mod n and u_2 = iw mod n
Step 5 Compute X = $u_1G + u_2Q$
Step 6 If x = 0 , reject signature
Otherwise compute v = x^{-1} mod n
Step 7 Accept signal only if v = i

3.3 Detectng Malicious Node

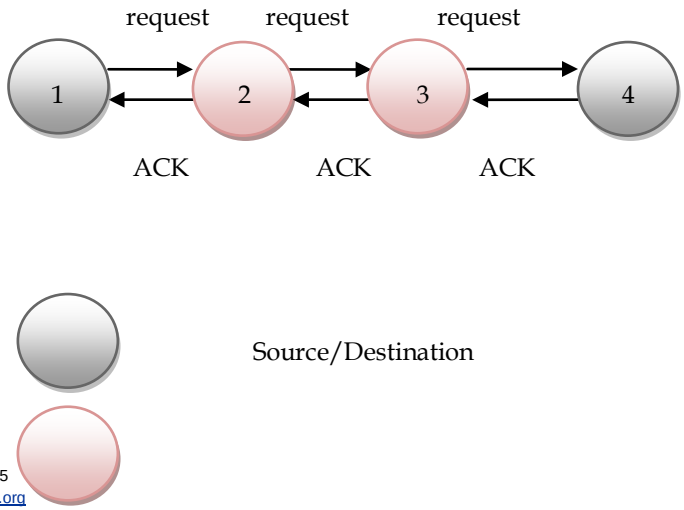
In this work malicious node act as a misbehaving node. So initially analyze the network and then detecting the malicious node . At first it will identify the malicious node in the network after that source node will send the message to all nodes in the network.

The proposed model assumes that N number of nodes is randomly arranged in the network. Node 1 is the source node and it transmits the data to the destination node through intermediary nodes. Here node 2 is the neighbour node of node N1. Node 1 forward the packet to node node 2. This process will continue until it reaches the destination node node 4.

Suppose the network identified that M is a malicious node and the node M will be blocked using elliptical curve cryptography algorithm so that forwarding of packet will not takeplace.

In the proposed system the public and private keys for every node are generated and distributed. Whenever the source node receives the acknowledgement ECC algorithm decrypts the acknowledgement and verifies the received acknowledgement time with the expected time. If there is a large delay in time then it assumes that it is because of some malicious activity so that the malicious node may not forward the packet to next node. Thus the chance of packet loss will be minimized.

Fig. 5 shows the packet forwarding in MANETs. Here S and D are the source and destination nodes. M is the malicious node. Initially S forward the packets to its immediate node 1 and node 1 forward the packet to its neighbor node until it reaches the destination.



Intermediary node

Fig.5 Normal Transmission

Steps with malicious nodes
Step1 : Initially network analyse the malicious node .
Step 2: Block the malicious node using ECC algorithm (section 3.2).
Step3: Choose an optimal path using fitness function.(section 3.4)

Fig.6 shows the packet forwarding in MANETs with malicious node. Here S and D are the source and destination nodes. M is the malicious node and node 1, 2 and 3 are the intermediary nodes. The network identified the malicious activity and block that node M using ECC. Finally it findout an alternate path S-2-3-D using fitness value.

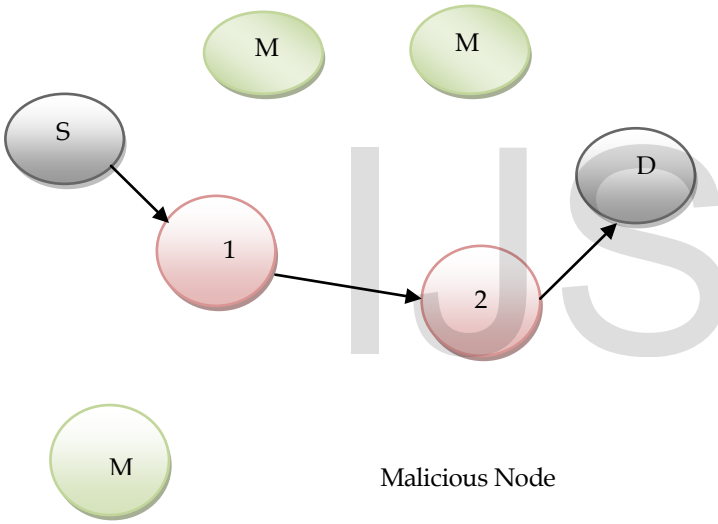


Fig.6 Network with malicious node

3.4 Identifying Optimal Path using Genetic Algorithm

Genetic algorithm is based on principles of evolution and natural selection. It is a search technique used in computing to find true or approximate solutions to optimization and search problems. Genetic Algorithm [13] can also be used to identify optimal path in wireless networks.

3.4.1 Parameters in Genetic Algorithm

There are many parameters to consider for the application of GA. Here discussing the basic parameters and the methodology.

Representation of a Chromosome

It's the initial phase. A chromosome represent a path which consist of sequence numbers.

Evaluation of fitness function

The fitness functions in the shortest path routing problem to find the minimal cost path and fitness of band-width [13].

Selection

Selection is the phase of genetic algorithm in which individual genomes are chosen from a population for later breeding. Individual solutions are selected through a *fitness-based* process. Most functions are stochastic and designed so that a small proportion of less fit solutions are selected.

Crossover

The point at which the chromosome is broken depends on the randomly selected crossover point. It is based on exchange between two fixed length chromosomes.

Mutation

After selection and crossover, a new population full of individuals is developed. This operator randomly alters genes to partially shift the search to new locations.

Elitism

A practical variant of the genetic process of constructing a new population is to allow the best organism from the current generation to carry over the next ,unaltered. It ensures the quality of the genetic algorithm will not decrease from one generation to next.

Reproduction

The next step is to generate a second generation population of solutions from those selected through genetic operators - crossover or mutation.

3.4.2 Architecture

The proposed algorithm worked as follows.

Step 1 : Create random initial population M and evaluate the cumulative and relative fitness function.
Step 2 : Apply Crossover:
2.1 Choose two solutions x and y from P_t based on the fitness values.
2.2 Using a crossover operator, generate offspring and add them to O_t
Step 3 : Mutate each solution $x \in O_t$.
Step 4 : Fitness Assignment: Assign a fitness value to each solution $x \in O_t$.
Step 5 : Selection: Select N solutions from O_t based on their fitness and assigned them $P_t + 1$.
Step 6 : If the stopping criterion is satisfied, terminate the search and return the current population, else, set t=t+1 go to Step 2.

Based on this fitness value it the optimal path is selected regardless of malicious node.

4 Performance Evaluation

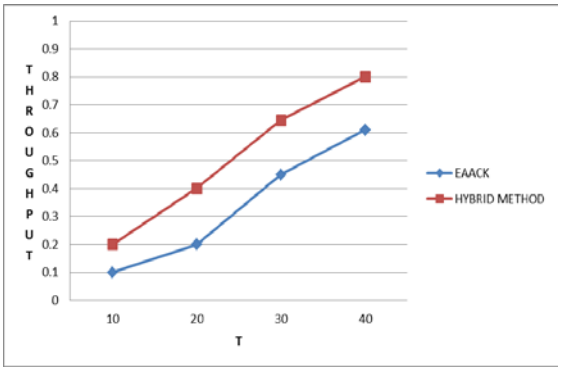
An experiment set up has done using Network Simulator 2 version 2.34 (ns-2). The default configuration of 10 to 40 nodes is considered in a flat space with size of 500 * 500. The packets are routed using AODV protocols. We use various metrics required for evaluation. These matrices are important because it analyse the performance of the network . The detailed simulation parameters are listed in the table 1.

TABLE 1
Simulation Setup

Simulation Parameters	Values
Channel Type	Wireless Channel
Propagation Model	Two Ray Ground
Network Interface Type	Phy/Wireless Phy
Interface Queue type	Queue/DropTail/PriQueue
Transmission Range	250m
Network Dimension	500*500
Queue capacity	40
MAC Protocol	IEEE 802.11
Antenna Type	Omni antenna

The performance of hybrid method is compared with one of the existing method EAACK. Here only one method is taken for comparison. Hybrid method shows comparatively better results than that of other traditional methods. The test shows that the proposed method has low end to end delay, high throughput and high packet delivery rate. Also the fitness value of each node is calculated. Based on the fitness value best path is selected.

Fig. 8, shows the comparison graph of throughput with one of the existing method named EAACK. X axis shows time and Yaxis shows Throughput. Hybrid method produce high throughput compared to that of the existing EAACK.



hroughput Vs Time

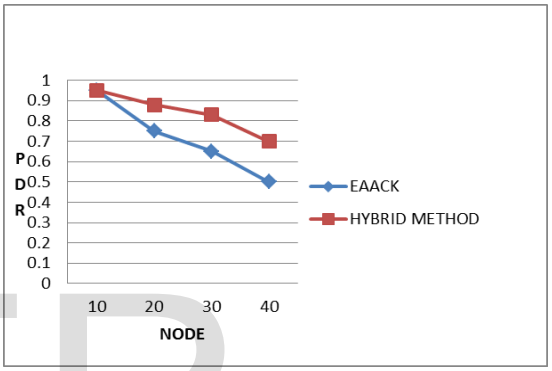


Fig.9 Packet deliver ratio Vs Nodes

Packet Delivery Ratio: It is the ratio of the number of packets delivered to the destination to the number of packets generated. Fig.9 shows the comparison of packet deliver ratio . It is found that the proposed method have high packet deliver ratio when compared to existing one.

$$PDR = \frac{\text{No. of packets received}}{\text{No. of packets sent}} * 100$$

5 Conclusion

Due to the the open nature and mobility mobile adhoc networks are more prone to malicious defects. The presence of these malicious activities has made to find an effective solution. A hybrid method consist of elliptic curve cryptography and genetic algorithm is proposed. In ECC points are generated from the elliptic curve of prime field and a point is chosen at random. When a set of nodes are ready to form a MANET, they authenticate and communicate with each other by using the private and public keys. The keys before sending and receiving must be signed at the sender and verified at the receiver. Elliptic curve digital signature algorithm is also adopted. Along with ECC, genetic algorithm is also used to find the optimal path from source to destination during second phase. Here relative fitness and cumulative fitness is evaluated. Based on this fitness value , best member is selected and optimal path is selected. By comparing the proposed method with baseline protocols, it is evident that

this hybrid method produce better performance during malicious node identification and optimal path identification.

REFERENCES

[1] A Karpijoki, "Security in Ad-hoc Network"', *Helsinki University of Technology, Tik-110.501 Seminar on Network Security, Telecommunications Software and Multimedia Laboratory*, 2000.

[2] Elhadi, Nan Kang and Tarek R. Sheltami, "EAACK—A Secure Intrusion-Detection System for MANETs", *IEEE Transactions on Industrial Electronics, Vol. 60, No. 3, March 2013* .

[3] Ming Chang, Po-Chun So S,Jiang Liang Chen, "CBDS A cooperative bait detection scheme to prevent malicious node for MANET based on hybrid defense architecture". *IEEE, 2011*.

[4] Marti, S., Giuli, T.J., Lai, K., Baker, "Mitigating routing misbehavior in mobile ad-hoc networks", *In: Proceedings of the 6th Annual International Conference on Mobile Computing and Net-working* pp. 255–265 (2000).

[5] Sheltami, A. Al-Roubaiey, E. Shakshuki, and A. Mahmoud, "Video transmission enhancement in presence of misbehaving nodes in MANETs,"*Int. J. Multimedia Syst.*, vol. 15, no. 5, pp. 273–282.

[6] Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems,"*Commun. ACM, vol* 21, no. 2, pp. 120–126, Feb. 1983.

[7] Saurabh Gupta, Subrat Kar, S Dharmaraja , "BAAP: Black hole Attack Avoidance Protocol for Wireless Network" *IEEE proceedings of the International Conference on Computer & Communication* .

[8] Nemoto and Nei Kato, " A Dynamic Anomaly Detection Scheme For AODV- Based Mobile AdHoc Networks", .*IEEE Transactions On VehicularTechnology*, Vol.58, No. 5, pp.2471-2481,June 2009.

[9] Gayoso Martínez, L. Hernández Encinas, and C. Sánchez Ávila, "A Survey of the Elliptic Curve Integrated Encryption Scheme," *Journal Of Computer Science And Engineering,* Volume 2, Issue 2 , Auguest 2010

[10] Gayoso Martinez, L. Hern´andez Encinas, and C. S´anchez´ Avila, "Java Card implementation of the Elliptic Curve Integrated Encryp tion Scheme using prime and binary finite fields", *Computational Intelligence in Security for Information Systems*, *Springer*, 2011.

[11] Nishu Garg, Mahapatra R.P, "MANET Security Issues," *IJCSNS International Journal of Computer Science and Network Security, Volume 9*, 2009, pp. 1-4.

[12] Menezes A, Okamoto T and VanstoneL S, "Reducing Elliptic Curve Logarithms to Logarithms in a Finite Field", *Journal of Information theory*, Volume 39, 1991, pp. 1639-1646.

[13] H. Goto, Y. Amounas and E. H. El Kinani "ECC Encryption and Decryption with a Data Sequence", *Applied Mathematical Sciences*,Vol. 6, 2012, no. 101, 5039 – 5047.

[14] T.Priyadharshini and Ar.Arunachalam, "Efficient Genetic Algorithm for Optimal Routing In Ad Hoc Networks," *International Journal of Advanced Research in Computer Science and Software Engineering,* Volume 3, Issue 2,February 2013

[15] Gihan Nagib And Wahied G. Ali, "Network Routing Protocol Using Genetic Algorithms", *International Journal Of Electrical & Computer Sciences IJECS-IJENS* ,Vol:10 No:02,Pages 40-44.