Mitigate Wormhole Attack and Blackhole Attack Using Elliptic Curve Cryptography in MANET

Mukul Shukla¹ · Brijendra Kumar Joshi² · Upendra Singh¹

Accepted: 15 June 2021 / Published online: 28 June 2021

© The Author(s), under exclusive licence to Springer Science+Business Media, LLC, part of Springer Nature 2021

Abstract

Numerous network can be connected by using the mobile ad hoc network. It can have security attacks like the worm hole, denial of service attack, jellyfish and also the blackhole. During this they take a path which is the shortest for the place where it has to reach. During sending of message two types of attacks are generally seen such as the blackhole attack and the wormhole attack. In this research we have tried to focus on two major attacks such as the black hole and the worm hole attack. In this we have used two types of protocol such as the AODV whose other name is SWBAODV and the scalable-dynamic elliptic curve cryptography. During the use the prime numbers are selected at random. We can also choose certain specific prime number. Moreover the security level does not depend on the size of the key. Keeping A as worm hole and B as the black hole we have made a two dimensional vector function named as $F[A, B]$. Two types of study is done by us in our research such as the with attack and without attack. In case of no attack study we have shown graphically using the AODV and the in case of attack we have given it as the BAODV and also the WAODV. Here we have applied a specific method SWBAODV to our selected attack case. The results were found to be interesting for the case of, packet delivery ratio and end to end delay was near 188.40 on comparing it with the BAODV and the WAODV. It has shown 51.38% more value compared to the BAODV and WAODV. There has been a drastic fall in the value of delay and it reached to a 63.2 for BAODV to WAODV. The other two things which we have discussed here is the consumption of energy and the overhead routing. The results in case of SWBAODV were good compared with the consumption of energy and save about 73.52% with the attacked case and around 69.35% with the routing done on the BAODV and WAODV. From our study we were able to say that it will give protection to the (MANET).

Keywords Wormhole attack · ECC · Mobile Ad-Hoc Network (MANET) · AODV · Blackhole attack · SWBAODV

✉ Upendra Singh
upendrasingh49@gmail.com

Extended author information available on the last page of the article

Fig. 1 Desing of the MANET

1 Introduction

The MANET is used without any network. The main benefit is that it can work where there is no wire link possible and also where there is very fast deployment.

It contains certain mobile nodes and base stations. It covers various sections such as the discovering routes, packet sending, communicating securely and also the monitoring of the network. It has to be protected against the attack and to do this a specific algorithm is made [1]. The multi hop fashion is used for the routing using the MANET. In both wire and wireless system we have to face certain problems like the face route failure. The main things are the mobility of nodes and the route failure in the MANET [2].

The design of the MANET can be seen from the Fig. 1 given above. The major challenge faced is the routing during the use of the MANET.

The method should be such that it can fight for the path link break under difficult conditions between the starting and the ending pint in the path during the communication [3].

Passive and active are the two types of attack seen in the MANET, The major attacks of our study here are the worm hole attack and the black hole attack.

BlackholeAttack: In this case the information such as the smalled route between the starting and the ending point are send in a wrong method. It is done by sending the RREP packets. The attck of black hole among the nodes twenty one and twenty two and also for thirty two and thirty three are seen in Fig. 2. This has to be taken care of and is very important in the ad hoc network. To stop this we have to find the malicious nodes and for that we have taken a algorithm which can help to stop this type of attack [4, 5].

Wormhole Attack: For this we have need two nodes which are malicious in nature. They keep track on all the activities happening. Then they decide and make a plan to attack the network by making a tunne. This is nearly impossible to detect and it also is a major attack. The method which we have suggested in our study will help to prevent this. The Fig. 2 shows the two nodes 11 and D shows the nodes which are malicious and are prepared by creating a tunne. The minimum nodes are required for the worm hole attack [1, 6].

Out of several algorithms none is usefull for the detection of attack. It is not taking care of such attacks. The algorithm whicch we have taken here will be help ful in the black hole and the worm hole attack. There is a speciality of our algorithm.

Figure 2 shows types of attacks like black hole, and worm hole. Blackhole attacks are capture packets and drop packets that way create a loss in whole networks. Worm-hole attack is the loss whole network through a tunnel, in this above figure denote W and Wh means wormhole attack, and B means blackhole attack. This figure has a total of 3

Fig. 2 Different types of attack by a Network Diagram

blackhole nodes and 2 wormhole attacks. In this scenario between source, the destination has four routes, but three routes are infected through the attacker, and only a single route is free that's why packet transmission using the proposed protocol follows the safe route between source to destination.

The two main purpose of our research are as follows.

- By using a cryptosystem with the elliptic curve and a key which is decreased he have made a scalable and dynamic cryptosystem.
- For resource oriented device the ECC is very important method.
- The ECDLP is dependent on the cryptosystem and is shown by the selection of the point base $G=(x, y)$, which is a reliable method. The big number order are given by G .
- The two main parameters on which it depends is the crypto system and the synchronization curve relating to both the links and which results in error.
- The security is dependent on two things such as the ECC security and the bonus and is done by selecting randomly the number which are prime.

The following is the scheme of the paper. In paper having five sections, respectively section introduction, literature review, proposed methodology, implementation and result, and final last section conclusion.

2 Literature Review

2.1 MANET and Attack on MANET Literature Review

[7] in which dlog is used to show two things. first the method to train and the second the method of glitch. this will help in two major things such as the network operation and its nodal attack and also the events which are abnormal. It has seven clusters and the rate of accuracy is around 96%.

[8] deals with the prevention of MANET by the black hole attack. They have prepared the method such as the ad hoc on demand vector for the routing and is applicable

for the black hole attack. It is used for the 2-opt algorithm. The local search used is the 2-opt for the algorithm. It increases the factors for the purpose of delivery ratio packet, sink and hops, delay on end to end basis.

[9] The Particle Swarm Optimization (PSO) algorithm is a special thing and can be defined by natural networks used for the detection of the intruder node. The researcher here deals with the communication delay, energy consumption and isolation of the intruder.

[10] Here we have tried to show the nodes which are seen in the mobile ad hoc network. They have been further divided into various classes.

[11] Deals with the two things: the Information-Centric Networking (ICN) and privacy in ICN literature and the questions related to it. The major areas are the risk of privacy, control access, mechanism of the enforcement and the threat to the security.

[12] Here we have tried to discuss the MANET and black hole attack. The two protocols used are the AODV and the DSR for two particular simulators such as the NS2 and the NS3. The results show that black hole attack reduces the end-to-end delay. The method of discovery route is reduced.

[13] Tried to discuss the wormhole attack which is very important in the MANET. In such cases a tunnel is created between the two nodes. There are two methods used for this: the active and passive.

[14] is used when there is two methods for reaching to the destination. The results are better in case of routing and delay and we also have used the algorithm.

[15] The method to prevent that is the self-cooperative trust (ESCT) algorithm and is used to protect the MANET. ESCT is used for the exchange of information and analyze the proper judgement. This is better suited to the network which is ad hoc and its parameter.

2.2 Elliptic Curve Cryptography and its Limitations

The Rivest Shamir Adleman (RSA) and the Diffie Hellman (DH) are the best among the two platforms for the MANET and are used for the crypto system and also for the Elliptic curve cryptography (ECC) for the reason of security [16].

There are two methods DH and RSA, and the minimal key required is the ECC and used for less consumption of power. They are applicable to many applications having orientation for the research [17–20]. In [17], ECC is for the 8-Bit Atmel processor.

In [19], the researchers have also discussed the ECC in the enhanced mode. And it can be used in the prime field (MSP430-16bit).

Reliable results are obtained and the efficiency in terms of ECC and micro controllers have low power. The two methods are used such as the 8-bit and the 256-bit and results are shown in Table 1.

Large keys are needed as the security parameters are used for the security of ECC and are also changing. For resource-oriented platform and even regular computers the size of the key is not important. There are many problems related to the user. In [21] NIST, for security issues proper curve is to be selected. The situation is more complicated when it lacks the user understanding and makes it inefficient in case of the security. The security issues are still there for the curve which is standard. In 2007 [22], in elliptic curve it increases the issues related to security.

Table 1 Secure montgomery curves

	$\rho - sec$	a	B	c
Curves	111	117,051	222	3
		486,661	255	19
		− 61,370	256	189
		− 240,222	256	765
		− 55,790	254	$-127 \times 2^{240} \times -1$
	192	2,065,150	383	187
	256	530,438	511	187

2.3 Dimensional Analysis

Here we have discussed the routing methods implemented for the attacks. Various methods have been implemented which are used in the research.

- **Drop (DR):** messages are dropped by the attackers
- **Modify and Forward (MF):** The field is changed by using the broad cast and the uni cast method for the routing message and the nodes at the neighbor hood.
- **Forge Reply (FR):** The wrong method of attack used for the RREP for the substitute of RREQ.
- **Active Forge (AF):** The transfer the wrong packet instead the RREP packet, and also identify the RREQ packet.

Goal set are also checked . The various types are given as follows.

- **Disruption of Route (RD):** The new route establishment is prevented and the present route is stopped.
- **Route Invasion (RI):** is used for the two nodes and then with out acknowledgemet the packets are dropped.
- **Node Isolation (NI):** routes from the nodes are broken..
- **Resource consumption (RC):** Is needed for the battery, space, band width consumption.

3 Presented Method

The ECC development issues and the resource oriented platforms are discussed here and tried to eliminate. The method is scalable and dynamics and discusses about the key size which is decreased. Here we have made a method to make more number of curves and also more security levels. This is related to the purpose of efficiency [23, 24, 24]. For security level 128,192,256 bits the curves are given here. In base field we have tried for better pseudo-Mersenne and arithmetic Montgomery-friendly. There are several constraints related to security [23], p-224, p-384, p-521 and is given by curves NIST. The safe and unsafe elliptic curves are also identified and the present curves can also be detected. Aranha et al. Two methods for efficiency and providing security are: Edward

curve and Montgomery curve (25,519) (1174). The equation showing both is given here $y^2 = x^3 + ax^2 + x$ and $x^2 + y^2 = 1 + ax^2y^2$ with prime $2^b - c$,

b and c are given here.;a, b, c are given Table 1 and shows the security of the curve. The two points are generated the base point and the initial point. The points required are deisgned accordingly. If we select the parameters related to the curve in a random manner it will be able to handle the loss due to security and loss done by small key.It is very useful in the processor with are simple and can be implemented there.

3.1 ECC and its Overview

Prime number is given by q and finite filed is given by F_q this is for three factors. $E|F_q$ show the curve which is on F_q and the result can be given by the equation $P = (x, y) (x, y \in F_q)$ reported suing Weierstrass $y^2 = x^3 + ax + b$, and has $a, b \in F_q$ and $4a^3 + 27b^2 \neq 0$, and O shows the point of ∞ . is $-P = (x, -y)$ is the inverse of P used near the point of symmetry. O is used to denote the abelian group, used for addition and doubling point operation. From this the problem related to the lograthim is discussed. [25] Hasse's is limited to the points over $E|F_q$, shown by the #E

$$q + 1 - 2\sqrt{q} \leq \#E \leq q + 1 + 2\sqrt{q} \quad (1)$$

Work on the $E|F_q$ can be seen using the closure property and gives the points over $E|F_q$. Here two point addition takes place geometrically i.e. P&Q using R as real number on the curve E, $E|R$ shows the point of intersection ad the curve is negative Pand Q. The line and the tangent are used for the case where P and Q are same. It starts doubling when it is added to itself. This rule is applicable to value of E everywhere. They are denoted in the cordirname form by this rules.

Point Addition P is given by $(x_1, y_1), Q = (x_2, y_2) \in E|F_q$, if $P, Q \neq 0, P \neq Q$ and $Q \neq -P$, using points related to $R=(x_3, y_3)$ and used of R in addition in $R=P+Q$ are given by the results in 2, 3 and 4.

$$x_3 = \lambda^2 - 2x_1 \quad (2)$$

$$y_3 = \lambda(x_1 - x_3) - y_1 \quad (3)$$

$$\lambda = (y_2 - y_1)/(x_2 - x_1) \quad (4)$$

Point Doubling P is expressed as $(x_1, y_1) \in E|F_q$ and $R = (x_3, y_3) = P + P$, given rise to the 4, 6 and 7 equation.

$$x_3 = \lambda^2 - 2x_1 \quad (5)$$

$$y_3 = \lambda(x_1 - x_3) - y_1 \quad (6)$$

$$\lambda = (3x_1^2 + a)/(2y_1) \quad (7)$$

The introduction of operation can be used for the scalar multiplication.

Scalar Multiplication In this $P = (x_1, y_1) \in E \mid F_q$, followed by k as integer. k and P are multiplied and are given by the kP , and are further added with P again for k more times. [26].

$$kP = (P + P + \dots + P) / k \quad (8)$$

P is used to denote the point order d and the results can be shown by $dP=0$. (Paar, [27] Lagrange's Theorem has been given in such a way that $\#E$ that it is been divided by d the integer. H is used to show the factor and can be got by $h=\#E/d$; the value of h is found to be less [27]. Pohlig-Hellman's [28] is used for the taking the advantage of this situation and is found the value is large for d . This is used for the creation of $ElFq$ (log problem which is discrete), and is given by Logarithm Problem for the Elliptic Curve Discrete (ECDLP).

ECDLP: For the two points here P & Q which are related to $ElFq$, we get an integer one and it is $1 \in [2, d-1]$ and $Q=IP$, for such type of integer.

The sub exponential time has relation with the algorithm [25]. We cannot crack such a crypto system and if has higher security compared to RSA.

In case of using same domain in advance we can use ECC. The integer a and b and F_q the finite field are shown in the curve where $P \in E \mid F_q$ and they select the value of P randomly. where cofactor is h and the order is d . We can also create the secret key by using the DH key and also the protocol for the exchange.

- (1) $k_a \in [2, d-1]$ is selected randomly, used for the calculation of $Q_a = k_a P$, and it is transmitted to the Party B Q_a .
- (2) similarly, from B we can create $k_b \in [2, d-1]$, used for the calculation of $Q_b = k_b P$, and yields the A Q_b .
- (3) A is used to compute the shared key as $Q_s = k_a Q_b$.
- (4) B is used to compute the shared key as $Q_s = k_b Q_a$.
- (5) For safe communication both A and B can be used and we can use both of them for the generation of key Q_s . Further it can be given by the protocol.
- (6) Let $M \in F_q$ has to be transmitted to A and also has to be given in B , M A can be used for encryption and for calculating $C = M + Q_s$.
- (7) M from C are used for decryption, and for the calculation of $M = C - Q_s$, by B .

3.2 Elliptic-Curve Cryptography Scheme Which is Dynamic and Scalable

3.2.1 Dynamically Assigning Parameter

The data related to different parameters are given in the Table 1. The curve for ECC using the scalable structure can be created by using three things a, b, c . It is related to the

Table 2 List. of curve

No	Parameter	Point
l_0	a_0, b_0, c_0, d_0, q_0	P_0
l_1	a_1, b_1, c_1, d_1, q_1	P_1
l_2	a_2, b_2, c_2, d_2, q_2	P_2
—	—	—
l_{L-1}	$a_{L-1}, b_{L-1}, c_{L-1}, d_{L-1}, q_{L-1}$	P_{L-1}

method of creating secure curve data. L shows the number of elliptical curve and is seen from the Table 2, integer is generated in random manner and is related to every curve. r l_i ($l_i \neq l_j \forall i \neq j$) for certain case of curves there i varies with in the limit of zero and till $L - 1$. Starting the curve from l_i , P_i is the starting place also d_i , shows its order with P_i . The conversation which is confidential is given by a curve.

The security of ECC is given by different signs and is denoted by the e [23] ρ -sec. 256 size is specified for the ECC key to attain 128 value of ρ -sec [23]. There are several problems associated with MANET. for showing strong curves ρ -sec values very higher so, there are values which are low are used ρ -sec, that is the ρ -sec curves has values in the limit of 128 also it is interchangeable and are given by ρ -sec curves having more than 110 bits and has the low values of bits. The efficiency will be more and the power consumption will be less in such cases. So to show that MANET is useful we have to select the communication curve which give more security and can cover the problem of key size and is given in Sect. 3.3.

There are various parameters which are stored randomly using the radio frequency identification tag which can be used for authentication and is the main reason behind the pseudonym throttling [29]. In this investigation we have tried to emphasize on the Polonium Authentication [30, 31]. With given request the pseudonym gives a tag and when visited it will begin from the starting. Curves can be described by the multiple set parameters. Upon request for every set there is a curve. They are sent in a proper order upon the request. From the Fig. 3 we can say that they can be executed by visiting the list.

3.2.2 Base Point Choice Arbitrary

For the construction of the cryptosystem the base point are more suitable and also are related to the ECDLP and are given by $G=(x, y)$ G must be there in as much as order which are there. For EC the method of representing is $\#E=\#d$, and it gives the value of base point d [27] and is given by first step in the algorithm. $P \in E | F_{q,w}$ here P are put on random basis. The G value is obtained from the Scalar multiplication of hP . The point at the base is taken as G for the case when neither G or dG are at infinity. When we need the parties of synchronization we can use both the parties and is given in our approach. Here we can keep the starting point as the P_i and for each curve l_i , and it gives proper value of G . The second algorithm gives the value of Montgomery Curves for the starting point. x_0 are selected randomly using F_q , and is given by $y_0 = x_0^3 + ax_0^2 + x_0 \bmod (2^b - c)$ if y_0

Fig. 3 Parameter synchronization protocol flow

a shows the residue quadratic of $\text{mod}(2^b - c)$ and (x_0, y_0) and are shown by the infinity point, the $\text{output}P_1(x_0, y_0)$ from the starting point.

From the starting the P is given and then the value of G is calculated from that.

Algorithm 1 Generating Base point

- 1: $P \in E | F_q$ for this select a random p .
- 2: perform scalar multiplication hP and suppose $G = hP$.
- 3: Identify $G \neq 0$. If not, go to 1.
- 4: Perform scalar multiplication dG .
- 5: Verify $dG = 0$. If not, go to 1.

Algorithm 2 Generating Initial Point

- 1: make random selection of element $x_0 \in F_q$.
- 2: Calculate $y_0 = x_0^3 + ax_0^2 + x_0 \text{mod}(2^b - c)$
- 3: Check if y_0 belongs to quadratic residue of $(2^b - c)$. If not, go to 1.
- 4: Check if (x_0, y_0) is the point of infinity. If it is, then go back to 1.
- 5: Output $P_1 = (x_0, y_0)$ as the initial point of 1.

3.2.3 Synchronization of Session Parameter

The ECDLP hardness and the synchronization curve gives he details of the crypto system. The decryption and the encryption method is dependent on the task of synchronization.. The can be helpful to reduce the system failure chance. Damage can be done by desynchronization so avoid this type of situation we have to create such a protocol that it will reset all the parameters. The figre 4 and 5 shows this type of situation.

The value are used for the further calculations. The steps like the +1 and -1 are calculated and followed by desynchronization. The perspective for the IoV, party A is used for Sensor(S), and is given by using B as Gateway(G) for both the study. the ID and ID' can also be used. C_f stores the last curve and the value of S&G are obtained from all the curves: C_f , C_c , and C_n ; The Cc states are used for the information related to synchronization. it is given by following three Eq. as 9, 10, and 11.

$$C_f = a_{i-1} || b_{i-1} || c_{i-1} || d_{i-1} || q_{i-1} || P_{i-1}^x || P_{i-1}^y \quad (9)$$

$$C_c = a_i || b_i || c_i || d_i || q_i || P_i^x || P_i^y \quad (10)$$

$$C_n = a_{i+1} || b_{i+1} || c_{i+1} || d_{i+1} || q_{i+1} || P_{i+1}^x || P_{i+1}^y \quad (11)$$

The results are given by the bits and are shown by $y ||$, the coordinates of x & y of points P are given by P_i^x and P_i^y Respectively. Figure 4 has been ud. to show the curves in G & S and from this we can get G_j^G and G_j^S ($j=f, c, n$), the and used for the synchroization of the flow of states and the protocol verification.

- (1) G is used for obtaining R form this value the value of verification information $G_1 = \text{hash}(C_c^G || ID || R)$.
- (2) G is used to sent the Query request $\{R, G_1\}$ to S .
- (3) For communication request can be done by S and used for the verification of the information $\{R, G_1\}$.
- (4) S calculates $S1 = \text{hash}(C_c^S || ID || R)$.

Fig. 4 Movement of limitation synchronization procedure

- (5) is used for the calculation of $G_1 = S_1$. If G_1 same as the S_1 , the curve parameter and the synchronization has been put for this purpose. i.e., C_c^S is the same as C_c^G , then S goes directly to Step 12. If G_1 is not same as S_1 , S and will go the following 6.
- (6) S is used for the calculation.
- (7) S is given by $G_1 = S_2$. If G_1 are same as S_2 , helps in the updation of the issues and also the value of G i.e., C_c^G are same C_f^S , then S has been seen in the following step 8. If has not specific way to go to Step 9.
- (8) Curve parameters can be updated using S by the following equation:
- (9) write back C_n^S as C_c^S .
- (10) write back C_c^S as C_f^S .
- (11) C_f^S is again generated for curve parameters and given by C_f^S ; goes directly by Step 12.

- (12) S are obtained by $S_3 = \text{hash}(C_n^S || ID || R)$ and followed by Step 10.
- (13) S checks if $G_1 = S_3$. If G_1 is equal to S_3 , and given by G and desynchronization are given by following i.e., C_c^G are related to C_n^S , then S is given by Step 11 shown the jump has no equality towards step 13.
- (14) S is used to show the upgrading parameter:
- (15) Writeback C_f^S as C_c^S ,
- (16) Writeback C_c^S as C_n^S ,
- (17) To obtain C_n^S by curve of parameter and we get the value of C_n^S ; for the step 12.
- (18) S is used for the generation of the value of $G S_4$

$$\text{where } S_4 = \text{hash}(C_c^S || ID').$$

- (19) S is used for the rejection information.

If S accepts the request for announcement, a procedure for confirmation will be carried out by G'

- (1) G gives the support of Information, and verification is done by $\{S_4\}$ using S .
- (2) G_2 calculation = $\text{hash}(C_c^G || ID')$ by G .
- (3) G is used to identify $G_2 = S_4$. If G_2 is same as S_4 , and S is used for the synchronization for the parameters of the curve, is further used for the curve synchronization.

The wrong attack or the desynchronization can also take place., and is further used for the G to S .

Figure 5 gives the method of the request for reset and is given by the following method.

- (1) A nonce M are used to obtain G are used to calculate $G_3 = \text{hash}(C_d^G || ID || M)$ is done.
- (2) G used for the method of send request, and is again used for the verification of the information. $\{M, G_3\}$ to S .
- (3) We get the demand by S also used for the verification of the information. $\{M, G_3\}$.
- (4) The method to calculate for $S_5 = \text{hash}(C_d^S || ID || M)$ was carried out by using S .
- (5) S is found to be correct if $G_3 = S_5$. If G_3 is same S_5 , and is said that for sending the request G and for the storing of curve G are similar for both the cases S , and the value of S is used for the 6th step; or, S and used for the 7th step.
- (6) For calculating $G S_6 = \text{hash}(C_d^S || ID')$ and also its sending is carried out by S .
- (7) information for the rejection is sent by S .

For the verification of request for reset the steps taken are as follows:

- (1) For calculating $G_4 = \text{hash}(C_d^G || ID')$ we have used G .
- (2) From G we can say if S_6 are equal to G_4 . For S_6 same as G_4 , it is proved that the information which is got from S is again stored in the S for the starting of the conservation. The information is taken as default and the conservation is also shut down.

For our protocol we have used the R randomly and also again G is given $C_c^G || ID || R$. and it is given by the sage alteration ($R, G1$); and implemented by thprotocol, request for the rejection is taken and the user S and also for the curve again taking as default. $G 1$

Fig. 5 Movement of the limitation reset protocol

cannot be used for learning and conversation cannot be built from d and the information which is forged is not obtained from S .

3.3 Performance and the Analysis

3.3.1 Proposed System and its Security Level

So the security level is given in [24], and can be given by the equation of the ρ -sec by the method of bits an EC.

$$S_o = \log_2 \left(\sqrt{\pi/4} \times \sqrt{\#E} \right) \quad (12)$$

Equation 12 shows the results:

$$S_o \geq \log_2 \left(\sqrt{\pi/4} \times \sqrt{q+1-2\sqrt{q}} \right) \quad (13)$$

$$\geq \log_2 \left(\sqrt{(\sqrt{q}-1)^2} + \log_2 \sqrt{\pi/4} \right) \quad (14)$$

The S_o has same value as the $\frac{B}{2}$, where $B = \lceil \log_2 q \rceil$ is given by integer q as bit length.

The key size is responsible for the selection of security so good security must be there. From Fig. 6 and NIST 2020 we can do estimation of the complexity complexity S_{er} for and is also given by random means using B .

$$S_{er} = \sqrt{\pi/2 \times B} \quad (15)$$

The value of complexity is getting doubled

$$S_{ee} = 2S_{er} = 2\sqrt{\pi/2 \times B} \quad (16)$$

The value of S_{com} is obtained by combining the bonus which we have got and the ECC security just by using a prime number.

$$\begin{aligned} S_{com} &= S_o + S_{ee} \\ &= \frac{B}{2} + 2\sqrt{\pi/2 \times B} \end{aligned} \quad (17)$$

Figure 7a gives the value of S_{ee} and S_o , wECC is used and nearly thirty percent increase is seen. The ρ -sec is calculated. From Fig. 7b remaining data are obtained. The results are given in 7b. As an example, 256-bit required size for the ECC and can be got by 128 bits for the ρ -sec. From Table 1 we can get the value of consideration of the curve and is found to be 192-bit, as ρ -sec of 34 is used for the additional security. The security for both is given by ρ -sec $(96+34)=130$ -bit, and is found to be more as 256-bit for the level of security of ECC.

Fig. 6 The additional security level and random prime number selection

(a) Enhancement of The Safety Level.

(b) Composite Security Level.

Fig. 7 Near by security for suggested approach

3.3.2 Analysis of Efficiency

ECC designed for the embedded system used for the execution time[17–20]. By using this method the performance can be improved.

256, 224, 192, 160, 128 bits is used to measure the crypto system by using the Micro ECC library [32], they efficiency can also be known by the key size. From the Fig. 8 we can see the efficiency improvement by the signature, verification and also by the key generation. Less time is required for the key generation. Also for making 192 bits for the 224 bits and also for the signature and the verification. The value for the reduction is 4.6 ms to 4 ms, 4 to 6 and 8 to 5 ms. The improvement in terms of percentage is about 33%, 31%, and 35%, and care has been taken that the security level is not reduced 1 to 4 times the execution of the function is done. Very fast results of the calculations can be obtained from the ECC. There is no need of extra time for the calculations. Both the approach the scalable ECC and the absolute resource are showing

Fig. 8 The curve efficiencies [33]

proper results. For the resource oriented system about 30% efficiency improvement values are used for the manet. [33].

3.3.3 Memory

The NIST curve shows how the ECC data are used. From the table we can obtain the value of. a, b, c, d, l_1 , q, and is given in Table 2. and also the Point P is given.. From curves L we can get the value of k1 to kt. Key size is used for the calculation..

$$K = \frac{\sum_{i=1}^t n_n k_i}{n} \quad (18)$$

So, bit size k for the E curve can be calculated for the $(7 * k/8 + 2)$ bytes along with L. For L=80 the size of the key is 160 bits, and required memory is around 1 KB. We are not concerned with the memory or the rate at which it is available.

3.3.4 Comparison Study

[18] For configurable ECC is serves as a library and the standard supporting are the 192,160,128; it is further used for the network of the sensor. [34] used MoTE curves which have low weight EC [35] MoTEECC is much flexible and is used for the library's purpose,256-bit, 224-bit, 192 bits, 160bit are the different types of the curve size associated with the field. The different versions for this are also tried our the trade off and to check the efficiency.

The prime field and the optimization of the arithmetic is given importance in this study. The study of efficiency and the power consumption is also carried out in our research. The original ECC method is used for the working of different configuration. Depending on the security system requirement the parameters are used such as the domain of the curve and this is fixed and public. From our study we can say that the problem of he single use curve for the intensive analysis is not face in the method which we have taken for our study.

Here, $k * P$ shows the time of execution in clock cycles which gives the scalar multiplication of the fixed base points. Tmote Sky* gives the version which is related to high speed., while Tmote Sky** which is also known as the efficiency version of memory. 256-bitkans 256-bitr respectively can be shown by the curve secp256r1 and curve secp256k1 and has been used ago.

We have made a study of the pre storage curve. We have use of the parameters for the dynamically by using the synchronization protocol. The time is reduced and the consumption and the optimization is done and is given in Table 3, This is applicable where there is constraints of the resources and also the change of the attack externally so to avoid this the method is used.

4 Result and Implementation

Blackhole Ad hoc On-Demand Distance Vector (BAODV), Wormhole AODV (WAODV), Ad hoc On-Demand Distance Vector (AODV) and Secure Wormhole and Blackhole AODV (SWBAODV) for all the effectiveness is checked. In NS2 a particular stimulation is developed for carrying out the experiments and to check the protocol related to the performance. We have compared all the algorithm and is efficiencies SWBAODV, AODV, BAODV, WAODV. It is applicable for the following energy and routing overhead, packet delivery ratio, end to end delay and throughput.

Table 3 Comparison the Performance of MICA, Tmote Sky, and this work

Security level ($\rho - sec$)	Platform	G.F. (p) field	$K * P$
80-bit	MICA _g	159-bit	2, 083, 000
	Tmote sky*	159-bit	1, 638, 000
	Tmote sky**	159-bit	1, 928, 000
	This work	128-bit	1, 590, 000
96-bit	MICA _g	191-bit	3, 338, 000
	Tmote sky*	191-bit	2, 433, 000
	Tmote sky**	191-bit	2, 910, 000
	This work	160-bit	2, 180, 000
112-bit	MICA _g	223-bit	5, 010, 000
	Tmote sky*	223-bit	3, 489, 000
	Tmote sky**	223-bit	4, 221, 000
	This work	192-bit	2, 910, 000
128-bit	MICA _g	255-bit	7, 159, 000
	Tmote sky*	255-bit	4, 798, 000
	Tmote sky**	255-bit	5, 864, 000
	This work	254-bit	4, 320, 000
144-bit	MICA _g	N/A	N/A
	Tmote sky*	N/A	N/A
	Tmote sky**	N/A	N/A
	This work	256-bit	7, 373, 000
	This work	256-bit	6, 294, 000

4.1 Experimental Simulation Tool

The results based on the NS2 mechanism are discussed here by the given algorithm.

4.1.1 Experimental Simulation Tool Setups

Processor: 11th Generation Intel, Core i5, Graphics: NVIDIA MX330 with 2 GB GDDR5, Solid State Drive: 512 GB, Ram: 8 GB, 1 × 8 GB, DDR4, 3200 MHz. Network Simulator 2 is install on Ubuntu 19.10.

The directory NS2.35 has been changed and the algorithm is used for the files like the ns-lib.TCL, Cmu-trace.cc, Cmu-trace.h, packet.h, ns-packet.TCL, Makefile, priqueue.cc, ns-agent.tcl, ns-mobilenode.tcl. Then commands are given and the following steps are taken.

4.1.2 Discussions and Results for NS2 Simulation

The comparative study was done for our algorithm WAODV, AODV, SWBAODV, BAODV for the packet delivery ratio, End to End Delay, protocols for throughput, proposed algorithm.

The simulation parameters are given in Table 4. Version of network is NS-2.35, simulation time in seconds (1000 s), Network size is 1500 m * 1500 m, 0.5 m /seconds to 9 m/s is maximum node speed, the data rate is CBR, and FTP, source, and destination are random, packet size of Data is 1024 bytes, Experimental set of protocol are WAODV, BAODV, AODV, and SWBAODV, IEEE 802.11, Propagation Two-ray ground for the propagation Model, random way point for the model of mobility, wireless channel is used for the channel type, antenna is apply Omnidirectional, Languages, AWK Scripting are Tcl, oTcl, C++, 50, 100, 150, 200 and 250 mobile nodes for simulation, are considered for group in our study and nearly 10% of the mobile nodes, i.e., 5, 10, 15, 20 and 25 respectively, come I in the network by wrong methods. This is applicable for the wormhole and the black hole attack. The graphs related to the wrong nodes and the scenario of the network are shown in this study.

Table 4 Simulation parameters

Parameters	Specification	Parameters	Specifications
Network simulator	NS-2, Version 2.35	PHY/MAC protocol	IEEE 802.11
Network size	1500 m × 1500 m	Propagation model	Two-ray ground
Connection protocol	TCP/FTP or UDP/CBR	Mobility model	Random way point
Data type	Constant Bit Rate (CBR) or File Transfer Protocol (FTP)	Channel type	Wireless channel
Source/description	Random	Antenna model	Omnidirectional
Data packet size	1024 bytes	Simulation time	1000 s
Simulation protocol	AODV, WAODV, BAODV, SWBAODV	Language	Tcl, oTcl, C++, AWK Scripting
Simulation Scinero (No. of Mobile node)	50, 100, 150, 200, 250	No of malicious nodes	5, 10, 15, 20, 25

4.2 Result

From the proposed approach we have arrived to certain data which are given here. From this the parameters related to the evaluation are given. The following are used routing overhead, packet delivery ratio, end delay ratio. The different types of nodes are discussed here and the details are given for the nodes 50, 100, 150, 200 and 250 in-network.

4.2.1 Throughput

The packets delivered per unit time successfully is given by the throughput parameter. Better results are obtained by secure AODV and are shown in the Fig. 9. They are compared with the blackhole attacked AODV and the Worm hole attacked AODV. The results show enhancement of 188.39 kbps.

The throughput reduces when it has been attacked. The method is used for the SWBAOV and the increase in throughput is seen.

4.2.2 End to end Delay

The end to end delay is the time for each packet to reach the source. The value of SWBAODV increases with the increase in the no of nodes and is shown in the Figs. 10 and 11. SWBAODV has better results compared to the WAODV and BAODV but it is less than AODV.

The overall delay can be reduced by the use of SWBAODV and it is seen by the comparison between the source and the scenario of attack.

4.2.3 Delivery Ratio for Packet

PDR means the packets and the ratio transmitted and the packet received by the source. There is an improvement and the results are given in the Figure 11. The improvement is

Fig. 9 Increase in no. of nodes against throughput

Fig. 10 E2E Delay, in term of 50,100,150,200,250 nodes

Fig. 11 Percentage of PDR in term of 50,100,150,200,250 nodes

around 51.38% for the attacked network while for the it is minimum for the AODV of the network based on PDR.

During the PDR network the number of wrong nodes are very much high and from our study we can see that there is a increase in the PDR.

4.2.4 Energy

Minimum energy consumption and the best results are seen with the SWBAODV when compared to the network which is attacked and the difference in the consumption is around 72.46%.

The use of proposed mechanism the reduced attack scenario will give better results for the SWBAODV.

4.2.5 Routing Overhead

Routing head is defined as the ratio of the packets transmitted to the packets which are received..

Secure approach is required for the SWBAODV and the results are shown in the Fig. 12 and 13. The results are 69.26% good with regards to the WAODV And the BAODV. The value is found to be 18.73 and is considered as very low.

5 Conclusion

The researcher are facing a challenge related to the platform and there has been a need to develop a micro controller type device and the sensor which has cryptographic platform which take into the problems related to the manet. They can give similar security like the RSA and the keys are also very few. The external analysis becomes easy by the use of the single curve. The scalable ECC which is dynamic is used here to solve

Fig. 12 Energy utilization percentage, in term of 50,100,150,200,250 nodes

Fig. 13 Routing overhead percentage in term of 50,100,150,200,250 nodes

the problem. Both the parties store the list. The list for different parties are discussed here. Extra security is required for the selection of the number and the curve on it. From the results it is seen that the consumption is reduced to a great extent. The parameters like the end to end delay, throughput, evaluation parameter and, are in the range of the 188.39 for both the BAODV and WAODV, i.e., increase about 51.37% over the BAODV and WAODV and decrease in delay around 63% from BAODV and WAODV. The routing over head and the energy consumption are also discussed here in details. The minimum consumption and that to around 72.45% saving was seen in the case of SWBAODV and was compared with attacked scenario and was found to be about 69.26% and was seen for the WAODV and BAODV. This proves very effective for the manet and safe guards it.

References

1. Elmahdi, E., Yoo, S. M., & Sharshembiev, K. (2020). Secure and reliable data forwarding using homomorphic encryption against blackhole attacks in mobile ad hoc networks. *Journal of Information Security and Applications*, 51, 102425. <https://doi.org/10.1016/j.jisa.2019.102425>
2. Moudni, H., Er-Rouidi, M., Mouncif, H., & El Hadadi, B. (2019). Black hole attack detection using fuzzy based intrusion detection systems in MANET. *Procedia Computer Science*, 151, 1176–1181. <https://doi.org/10.1016/j.procs.2019.04.168>
3. Kalkha, H., Satori, H., & Satori, K. (2019). Preventing black hole attack in wireless sensor network using HMM. *Procedia Computer Science*, 148, 552–561. <https://doi.org/10.1016/j.procs.2019.01.028>
4. Tsiota, A., Xenakis, D., Passas, N., & Merakos, L. (2019). On Jamming and black hole attacks in heterogeneous wireless networks. *IEEE Transactions on Vehicular Technology*, 68(11), 10761–10774. <https://doi.org/10.1109/TVT.2019.2938405>
5. Vinayagam, J., Balaswamy, C., & Soundararajan, K. (2019). Certain investigation on MANET security with routing and blackhole attacks detection. *Procedia Computer Science*, 165, 196–208. <https://doi.org/10.1016/j.procs.2020.01.091>

6. Patel, M., Aggarwal, A., & Chaubey, N. (2020). *Analysis of Wormhole Detection Features in Wireless Sensor Networks* (pp. 22–29). Springer, Cham
7. Li, T., Ma, J., Pei, Q., Song, H., Shen, Y., & Sun, C. (2019). DAPV: Diagnosing Anomalies in MANETs Routing with Provenance and Verification. *IEEE Access*, 7, 35302–35316. <https://doi.org/10.1109/ACCESS.2019.2903150>
8. Keerthika, V., & Malarvizhi, N. (2019). Mitigate black hole attack using hybrid bee optimized weighted trust with 2-Opt AODV in MANET. *Wireless Personal Communications*, 106(2), 621–632. <https://doi.org/10.1007/s11277-019-06182-8>
9. Kavitha, T., Geetha, K., & Muthaiah, R. (2019). India: Intruder node detection and isolation action in mobile ad hoc networks using feature optimization and classification approach. *Journal of Medical Systems*. <https://doi.org/10.1007/s10916-019-1309-2>
10. Gurung, S., & Chauhan, S. (2019). A survey of blackhole attack mitigation techniques in MANET: Merits, drawbacks, and suitability. *Wireless Networks*. <https://doi.org/10.1007/s11276-019-01966-z>
11. Tourani, R., Misra, S., Mick, T., & Panwar, G. (2018). Security, Privacy, and Access Control in Information-Centric Networking: A Survey. In *IEEE Communications Surveys and Tutorials* (Vol. 20, Issue 1, pp. 556–600). Institute of Electrical and Electronics Engineers Inc. <https://doi.org/10.1109/COMST.2017.2749508>
12. Ochola, E. O., Mejale, L. F., Eloff, M. M., & Van Der Poll, J. A. (2017). Manet reactive routing protocols node mobility variation effect in analyzing the impact of black hole attack. *SAIEE Africa Research Journal*, 108(2), 80–91
13. Sankara Narayanan, S., & Murugaboopathi, G. (2020). Modified secure AODV protocol to prevent wormhole attack in MANET. *Concurrency Computation*, 32(4) e5017
14. Yaseen, Q. M., & Aldwairi, M. (2018). An enhanced AODV protocol for avoiding black holes in MANET. *Procedia Computer Science*, 134, 371–376. <https://doi.org/10.1016/j.procs.2018.07.196>
15. Cai, R. J., Li, X. J., & Chong, P. H. J. (2019). An evolutionary self-cooperative trust scheme against routing disruptions in MANETs. *IEEE Transactions on Mobile Computing*, 18(1), 42–55. <https://doi.org/10.1109/TMC.2018.2828814>
16. Agency, S. B. (2014) The Case for Elliptic Curve Cryptography. <http://www.nsa.gov/ia/industry/crypto/elliptic.curve.cfm>
17. Gura, N., Patel, A., Wander, A., Eberle, H., & Shantz, S. C. (2004). Comparing elliptic curve cryptography and RSA on 8-Bit CPUs. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 3156, 119–132. https://doi.org/10.1007/978-3-540-28632-5_9
18. Liu, A., & Ning, P. (2008). TinyECC: A configurable library for elliptic curve cryptography in wireless sensor networks. *Proceedings- 2008 International Conference on Information Processing in Sensor Networks, IPSN 2008*, 245–256. <https://doi.org/10.1109/IPSN.2008.47>
19. Wang, H., & Li, Q. (2006). Efficient implementation of public key cryptosystems on mote sensors. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 4307 LNCS, 519–528. https://doi.org/10.1007/11935308_37
20. Wenger, E. (2013). Hardware architectures for MSP430-based wireless sensor nodes performing elliptic curve cryptography. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. LNCS, 7954, 290–306. https://doi.org/10.1007/978-3-642-38980-1_18
21. Locke, G., & Gallagher, P. (2009). FIPS PUB 186–3 Digital Signature Standard (DSS) Category: Computer Security Subcategory: Cryptography.
22. Bernstein, D. J., & Lange, T. (n.d.). *Security dangers of the NIST curves*. Retrieved March 28, 2020, from <http://xkcd.com/927>
23. Aranha, D. F., Barreto, P. S. L. M., Pereira, G. C. C. F., & Ricardini, J. E. (2013). A Note on High-Security General-Purpose Elliptic Curves. *IACR Cryptology ePrint Archive*.
24. Bos, J. W., Costello, C., Longa, P., & Naehrig, M. (2016). Selecting elliptic curves for cryptography: An efficiency and security analysis. *Journal of Cryptographic Engineering*, 6(4), 259–286. <https://doi.org/10.1007/s13389-015-0097-y>
25. Silverman, J. H. (2009). *The Arithmetic of Elliptic Curves* (Second Edition). In *Springer* (Vol. 106). Springer-Verlag New York. <https://doi.org/10.1007/978-0-387-09494-6>
26. Hankerson, D., Menezes, J. A. & Vanstone, S. (2006). Elliptic Curve Arithmetic. In *Guide to Elliptic Curve Cryptography* (pp. 75–152). Springer-Verlag. https://doi.org/10.1007/0-387-21846-7_3
27. Paar, C., & Pelzl, J. (2010). *Understanding Cryptography*. In *Understanding Cryptography*. Springer, Berlin Heidelberg.

28. Pohlig, S. C., & Hellman, M. E. (1978). An improved algorithm for computing logarithms over GF(p) and Its cryptographic significance. *IEEE Transactions on Information Theory*, 24(1), 106–110. <https://doi.org/10.1109/TIT.1978.1055817>
29. Juels, A. (2005). Minimalist cryptography for low-cost RFID tags (extended abstract). *Lecture Notes in Computer Science*, 3352, 149–164. https://doi.org/10.1007/978-3-540-30598-9_11
30. Lynch, T. (2007). Symbiotic Host Authentication and Identification, US Patent App. 11/685,671.
31. Wong, R. M., Berson, T. A., & Feiertag, R. J. (2012). Polonium: An identity authentication System. *Proceedings-IEEE Symposium on Security and Privacy*, 2012, 101–107. <https://doi.org/10.1109/SP.1985.10001>
32. Mackay, K. (2017). Micro ECC, kmackay.ca/micro-ecc/. [Access on 04.11.2017].
33. Wang, J., Li, J., Wang, H., Zhang, L. Y., Cheng, L. M., & Lin, Q. (2019). Dynamic scalable elliptic curve cryptographic scheme and its application to in-vehicle security. *IEEE Internet of Things Journal*, 6(4), 5892–5901. <https://doi.org/10.1109/JIOT.2018.2869872>
34. Liu, Z., Huang, X., Hu, Z., Khan, M. K., Seo, H., & Zhou, L. (2017). On emerging family of elliptic curves to secure internet of things: ECC comes of age. *IEEE Transactions on Dependable and Secure Computing*, 14(3), 237–248. <https://doi.org/10.1109/TDSC.2016.2577022>
35. Liu, Z., Wenger, E., & Großschädl, J. (2014). MoTE-ECC: Energy-scalable elliptic curve cryptography for wireless sensor networks. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 8479 LNCS, 361–379. https://doi.org/10.1007/978-3-319-07536-5_22

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Mukul Shukla is an Associate Professor in Information Technology at Shri Govindram Seksaria Institute of Technology and Science, Indore (M.P.), India. His research interests are IoT, Mobile adhoc and Wireless Sensor Networks. He has number of research papers to his credit. He has **granted** three **Indian Patent** on smart helmet, a system for detection and tracking of suspicious persons in crowd and a smart vehicle. He has published two Indian Patent on a system and method for detecting malicious activities in computing network and an intelligent system to detect covid-19 protocols. He has 15+ years of teaching experience.

Brijendra Kumar Joshi is a Professor in Electronics & Telecommunication and Computer Engineering at Military College of Telecommunication Engineering, Mhow (M.P.), India. He has completed B.E. in Electronics and Telecommunication Engineering from Govt. Engineering College, Jabalpur, M.E. in Computer Science and Engineering from IISC, Bangalore, Ph.D. in Electronics and Telecommunication Engineering from Rani Durgavati university, Jabalpur and M. Tech in Digital Communications from MANIT, Bhopal. His research

interests are Programming Languages, Compiler Design, Digital Communications, Mobile adhoc and Wireless Sensor Networks, Signal Processing, Parallel Computing and Software Engineering. He has number of research papers to his credit and has supervised three PhD scholars and currently supervising eight PhD scholars. He has published two books on Data Structures and Algorithms with Tata McGraw-Hill. He has 30 years of teaching experience.

Upendra Singh is an Assistant Professor in Information Technology at Shri Govindram Seksaria Institute of Technology and Science, Indore (M.P.), India. He has completed B.E. in Information Technology from Shri Govindram Seksaria Institute of Technology and Science, Indore, M.Tech. in Computer Science and Engineering from Rajiv Gandhi Proudyogiki Vishwavidyalaya, Bhopal, His research interests are Data Mining, Cloud, Machine Learning, Mobile adhoc and Wireless Sensor Networks. He has number of research papers to his credit. He has **granted** three **Indian Patent** on smart helmet, a system for detection and tracking of suspicious persons in crowd, and a smart vehicle. He has **published** five **Indian Patent** on an intelligent system to detect covid-19 protocols, a system and method for detecting malicious activities in computing network, smart autonomous weed detector and removal, iot – ai/ml-based vehicle direction-assistance system, and road asset management system. He has 5 years of Industry experience. He has 2 year of teaching experience.

Authors and Affiliations

Mukul Shukla¹ · Brijendra Kumar Joshi² · Upendra Singh¹

Mukul Shukla
mukulrshukla@gmail.com

Brijendra Kumar Joshi
brijendrajoshi@yahoo.com

¹ Shri Govindram Seksaria Institute of Technology and Science, Indore, India

² Military College of Telecommunication Engineering, Mhow, India