Elliptic Curve Digital Signature technique based Abnormal Node Detection in Wireless AD HOC Networks

P Deepalakshmi\textsuperscript{1} and T Kumanan\textsuperscript{2}

\textsuperscript{1,2}Department of Computer Science and Engineering, Meenakshi Academy of Higher Education and Research Chennai, India\textsuperscript{1}deepla.mca85@gmail.com

Abstract. This Security, as well as routing Performance, is two significant operations of Wireless ad-hoc networks (WANETs). Even though, several efforts to enhance its secure routing scheme of WANETs continue susceptible to attacks. Contrasting the majority of conventional solutions which avoid the precise problems, this scheme inclines to distinguish the misconduct as well as recognize the abnormal nodes in WANETs. In this paper, the Elliptic Curve Digital Signature technique (ECDST) is used to detect the abnormal node in the WANET. This technique function recognizes the abnormal node as well as isolate that node them from the route. During route discovery, the ECC method utilizing the Weierstrass Elliptic functions for detecting the abnormal node. The abnormal nodes are discovered by signature verification technique on data communication. It attains consistency in routing with disqualifying the link by the utmost weight as well as validates the nodes. This scheme assures node availability, integrity, as well as improves network performance. The observational analyses illustrate that the introduced scheme can notice the abnormal as well as a compromised node in the network.

Keywords: Wireless Ad-Hoc Networks, Reliability, The Weierstrass Elliptic Function, Elliptical Curve Digital Signature Technique, Security, Abnormal Node Detection.

1. Introduction
WANET is a self-structured multi-hop system constituted through several mobile wireless nodes with peer-to-peer association. WANET cannot have present communications as well as wireless nodes that travel robustly lacking edge restrictions [1]. Benefits are speedy to establish, allowance fault acceptance, association as well as movement. Though, the WANET’s disputes are active topography, unlock medium, embarrassed bandwidth, changeable capacity connections, energy-restrained function as well as imperfect physical security [2]. The absent of central administration as well as dependable wireless connection, susceptibility, safety coercion conducts to enhance the security. It routinely persists from attacks by self-interested otherwise abnormal nodes. For instance, irregularity actions attack, on-off attack, black hole attack, badness mouthing attack, grey hole attack and so on [3].

To overcome the above difficulty, we pertain an Elliptic Curve Digital Signature technique (ECDST) is used to detect the abnormal node in the WANET. This technique function recognizes the abnormal node as well as isolate that node them from the route. During route discovery, the ECC method utilizing the Weierstrass Elliptic functions for detecting the abnormal node. The abnormal nodes are discovered by
signature verification technique on data communication. It attains consistency in routing with disqualifying the link by the utmost weight as well as validates the nodes. The stay of this work is prepared as follows. In Section 2, the related work is surveyed. The ECDST is depicted in Section 3. In Section 4, present performance analyses. At last, finish in Section 5.

2. Related works
First, Energy awake trust scheme [4] is provide sufficient security as maintain overhead by utilizing a game theoretic technique. This technique is functional to the trust origin method to diminish the overhead. Although this scheme enhances the overhead of routing in the network. Key distribution scheme adapt secure property by giving pair wise keys among nodes. Secure Connectivity scheme inquire the results of key distribution possibility on route length, queue size, and energy looseness while minimal cost routing is employed [5]. Authentication enables a node to ensure the identity of peer node. Authentication is essentially assured that participants in communication are authenticated and not impersonators. Authenticity is ensured because only the legitimate sender can produce a message that will decrypt properly with the shared key [6].

A trust based security protocol that reaches authentication of data packets. In this scheme, every node keeping trust counter for observing and separating the malevolent node in the network [7]. However, this scheme cannot provide confidential data transmission in the network. A key agreement scheme based on public discussion was described that attain a convinced secret key range while an opponent has more favourable situation. A secret key agreement protocol introduced the reliable relay regarded in the discourse to attain both reward distillation and secrecy elaboration [8].

Throughput is enhanced with data-aided valuation method by means of transmit choice, channel then transmit obligation [9]. Masquerading Attack detection system (MADS) using the received signal-strength (RSS). In this method, the Signal strength variation is used to detect the attack accurately. The RSS is a lightweight cryptographic certification that as well does not necessitate extra charge to the present wireless technology. Although, the RSS is not quite authentic since it changes as well as fluctuates over time owing to several elements, for example multipath passing, deflection, etc. [10].

Numerous key management approaches inserted to initiate symmetric keys [11]. This approach applying arbitrary seed dissemination with transient master key which offer pair wise keys. This approach discovers the main disadvantage is providing less security.

3. Proposed systems
In this approach, the ECDST is applied for recognizing abnormal nodes in WANET. It contains normal nodes, as well as abnormal nodes. Figure 1 illustrates the network Structure of approach Scheme. This approach comprises three parts such as generation of key, generation of signature, also verification of signature.
3.1. Secure Route Discovery
The ECC method is utilizing the Weierstrass Elliptic purpose. Conceive the co-ordinate points of the sender as well as the Next relay node R be E as well as F correspondingly; there is another point G that makes a straight line as exemplified in the figure 2.

Figure 1. Network Structure of ECDST approach

Figure 2. Elliptic Curve
The Weierstrass Elliptic procedure is defined in (3),

\[ y^2 = x^3 + lx + m \]  

(3)

Where \( E + F = G \) \( \forall E, F \in G \)  

(4)

\( E \neq F \) and \( \forall E, F \in G \)

Where \( (x_E, y_E) \) and \( (x_F, y_F) \) and \( (x_G, y_G) \) are the coordinates of the E, F and G points forming an elliptic curve. Therefore, the co-ordinates \( (x_G, y_G) \) can be obtained from the following expressions,

\[ x_G = \beta^2 - x_E - x_F \]  

(5)

\[ y_G = \beta(x_E - x_G) - y_E \]  

(6)

where, \( \eta = \frac{y_F - y_E}{y_F - y_E} \)

The independent property of this procedure states that,

\[ E + F = F + G \]  

(7)

For the moment, the Source generated key \( (S_{\text{key}}) \) is evaluated utilizing expression (8) and the next relay node responds to with the \( R_{\text{key}} \) by the expression (9).

\[ S_{\text{key}} = E + F \]  

(8)

\[ R_{\text{key}} = F + G \]  

(9)

During route discovery, the source S equates its \( S_{\text{key}} \) with the \( R_{\text{key}} \) to finish that the next relay node is an abnormal node. When \( S_{\text{key}} \) is not equal as \( R_{\text{key}} \) next the node is available as an abnormal and it broadcast the whole network.

### 3.2. Generation of key Part

The ECDS factors are depicted as: \( T = (Fp, EC, C, H, m, k, R) \), where \( Fp \) is the finite field, \( EC \) represents the curve of elliptic, \( C \) denotes the point of Creator, \( m \) is the order of \( C \) a great prime number as well as \( k \) is coefficient factor. This approach applies a hash function \( H \).

In addition, data communication, the source checks the abnormal based on the ECDS confirmation method. If the node succeed the signature verification next it communicates the data to the destination otherwise transmit the abnormal node details to whole network as well as eliminate that node from the WANET.

### 3.3. Generation of signature Part

The source picked out an arbitrary number \( A_s \) among 1 to \( m - 1 \) that represents a private key \( PR_k \) as well as it Calculates its public key \( PU_k = C, A_s \). For every node \( j \), the source creates an arbitrary number \( \gamma \) among 1 < \( \gamma \) < \( m - 1 \). It calculates public key for every node \( PU_j = C, \gamma_j \). The source builds a signature for every node applying signature function \( s_j(\gamma_j, ID, A_s) \) is given below.

\[ S_j = \gamma_j^{-1}[\gamma_j k(ID) + A_s] \]  

(10)

Every node is payload with its precise signature \( S_j \), public credential of source \( A_s \), as well as public credential of every node \( \gamma_j \) is prepared public to the WANET.

### 3.4. Signature verification part

This part verifies through the node to make sure which the signature \( s_j \) concerns to it as well as has been accurately yielded. The node applies its node identity, public credential, as well as the public credential of the source to confirm the accuracy of the node \( j \) signature.
\[ S_j = \gamma_j^{-1}[\gamma_j, k(ID) + A_i] \]  

(11)

\[ \gamma_j = S_j^{-1}[\gamma_j, k(ID) + A_i] \] Reproduce all part with C

\[ C \cdot \gamma_j = C \cdot S_j^{-1}[\gamma_j, k(ID) + A_i] \]

\[ S_j^{-1} C \cdot \gamma_j \cdot k(ID) + S_j^{-1} C \cdot A_i \]

\[ C \cdot \gamma_j = S_j^{-1} \cdot k(ID) \]. Public certificate of node j+ sj−1 and public credential of the source and Node j confirms its signature value Sj as certain at (1) by calculating the RHS significance of expression (11) also calculating it with LHS. If the expression (11) is fulfilled next the signature of node j is confirmed. This process is attempted through the other nodes in a same way.

Figure 3. ECDS Confirmation method

The Figure 3 illustrates the ECDS confirmation between nodes. Here, the signatures of source as well as entire nodes are verified, except the signature of node d. Then, the source disseminates the notification message to WANET. This double checking process accurately detects the abnormal node in the WANET.

4. Performance Evaluation
To execute simulation examination, we utilized the NS-2.35 that incorporates the 802.11 MAC protocol. The packet traffic is yielded with constant bit rate. This simulation examination, we measured the following metrics namely Packet Obtained Rate, Latency, Loss Packet Rate, Average Remaining Energy, Throughput as well as detection ratio.

4.1. Packet Obtained Rate(POR)
It is defined as the ratio among the amount of data packets perfectly obtained by the receiver and the amount of data packets yielded by entire mobile nodes.
From this figure 4, the proposed method ECDST is greater compare to the existing method MADS. Since, the ECDST pick the route by the normal nodes. Thus, enhances the routing efficiency.

4.2. Packet Drop Rate (PDR)

It is denoted as the distinction among the forward packets and obtained packets in the communication WANET per particular time. PDR is measured by Equation 13.

$$\text{PDR} = \frac{\sum_0^n \text{Forward Packets} - \text{Obtained Packets}}{\text{Time}}$$  \hspace{1cm} (13)

From figure 5 illustrate the PDR of ECDST and MADS. The ECDST method selects the relay node by signature verification algorithm. Thus, reduces the network PDR in the system.
4.3. Packet Drop Rate (PDR)

It is defined as the time period from while the data packet communication is initiated at the source to while the data packet is perfectly obtained by the destination. We evaluated both its usual value and its allotment.

\[
Latency = \sum_{0}^{n} (\text{Packet Obtained Time} - \text{Packet Forward Time})
\]  \hspace{1cm} (14)

![Figure 6. Latency of ECDST and MADS](image)

The figure, 6 illustrates the latency of ECDST and MADS. The data traverse via link normal behavior nodes. Thus minimizes the routing latency.

4.4. Packet Drop Rate (PDR)

It is the vital parameter for measuring the operations of network. In this protocol, the throughput is specified as the amount of data packets effectively obtained at the receiver.

\[
\text{Throughput} = \frac{\sum_{0}^{n} \text{Packets Received}(n) \ast \text{Packet size}}{\text{Time}}
\]  \hspace{1cm} (15)
Figure 7. Throughput of ECDST and MADS of ECDST and MADS

The figure 7 proves the ECDST scheme has higher throughput. Because of, MADS scheme concentrate mainly the RSS. But, ECDST focuses the node reliability by elliptical curve Weierstrass function and elliptical curve digital signature thus ECDST has provide better performance in WANET.

4.5. Detection Ratio

Here, we observe the ECDST and MADS routing protocol detection ratio. The detection ratio is determined as given below WANET.

\[
Detection Ratio = \frac{Detected \ nodes}{Whole \ nodes}
\]  

(16)

Figure 8. Detection Ratio of ECDST and MADS

The detection ratio of ECDST and MADS protocols are projected in Figure 8. During route discovery, the Weierstrass Elliptic function is used to detect the abnormal nodes in ECDST. It illustrates that the detection rate of ECDST is better than MADS protocol due to the signature verification method distinguish the abnormal nodes in the WANET.
5. Conclusion
In this paper, we proposed Elliptic Curve Digital Signature technique based Abnormal Node Detection in WANET. This approach observes the abnormal nodes as well as it offers reliable data communication in the WANET. During route discovery, the ECC method is utilizing the Weierstrass Elliptic function for detecting the abnormal node. The abnormal nodes are discovered by signature verification technique on data communication. Thus, it renders better consistency as well as expands the network function while equating to the existing MADS approach. Our simulation outcomes illustrate that this approach offers assured packet obtained rate, enhances both the throughput, as well as detection ratio also dilutes the latency in the WANET.

References
[1] Umamaheswari S and Radhamani G 2015 Enhanced ANTSEC framework with cluster based cooperative caching in mobile ad hoc networks Journal of Communications and Networks 17 40-46
[2] Canêdo D R C and Romariz A R S R 2019 Intrusion Detection System in Ad Hoc Networks with Artificial Neural Networks and Algorithm K-Means IEEE Latin America Transactions 17 1109-1115
[3] Poongodi T, Khan MS, Patan R, Gandomi A H and Balusamy B 2019 Robust Defense Scheme Against Selective Drop Attack in Wireless Ad Hoc Networks IEEE access 7 18409-18419
[4] Duan J, Gao D, Yang C, Foh CH and Chen HH 2014 An energy-aware trust derivation scheme with game theoretic approach in wireless sensor networks for IoT applications IEEE Internet of Things Journal 1 58-69
[5] Yildiz HU, Ciftler BS, Tavli B, Bicakci K and Incebacak D 2016 The impact of incomplete secure connectivity on the lifetime of wireless sensor networks IEEE Systems Journal 12 1042-1046
[6] Lingeshwari S and Natchadalingam 2014 Provisioning of Efficient Authentication Technique for Implementing in Large Scale Network Int. Journal of MC Square Scientific Research 6 34-42
[7] Patil KT and Patil ME 2014 Improve the Security of CGA using Adjustable Key Block Cipher based AES, to Prevent Attack on AES in IPV6 over MANET IEEE Global Conf. on Wireless Computing & Networking 148-152
[8] Wang N, Zhang N and Gulliver TA 2013 Cooperative key agreement for wireless networking: Key rates and practical protocol design IEEE Transactions on Information Forensics and Security 9 272-284
[9] Santhakumar R 2017 Resource Allocation in Wireless Networks by Channel Estimation and Relay Assignment Using Data-Aided Techniques,” International Journal of MC Square Scientific Research 9 40-47
[10] Abbas S, Faisal M, Rahman HU, Khan MZ and Merabti M 2018 Masquerading Attacks Detection in Mobile Ad Hoc Networks IEEE Access 6 55013-55025
[11] Gandino F, Montrucchio B and Rebaudengo M 2013 Key management for static wireless sensor networks with node adding IEEE Transactions on Industrial Informatics 10 1133-1143