(12) PATENT APPLICATION PUBLICATION (21) Application No.202211044328 A

(19) INDIA

(22) Date of filing of Application :03/08/2022 (43) Publication Date : 19/08/2022

(54) Title of the invention : TRUST AWARE INTRUSION DETECTION SYSTEM BASED ON CLUSTER

(51) International classification	:H04L0029060000, H04W0084180000, H04W0012120000, H04W0040200000, H04W0012100000
(86) International Application No Filing Date	:NA :NA
(87) International Publication No	: NA
(61) Patent of Addition to Application Number Filing Date	:NA :NA
(62) Divisional to Application Number Filing Date	:NA :NA

(71)**Name of Applicant :**
1)Dr.Devendra Singh
Address of Applicant :Associate Professor, Department of Computer Science and Applications Engineering, SSCA, IFTM University Moradabad, UP 244001 Moradabad ----------- -----------
2)Dr. Anil Kumar
3)Mr. Ankur Chahal
4)Dr.Rahul Kumar Mishra
Name of Applicant : NA
Address of Applicant : NA
(72)**Name of Inventor :**
1)Dr.Devendra Singh
Address of Applicant :Associate Professor, Department of Computer Science and Applications Engineering, SSCA, IFTM University Moradabad, UP 244001 Moradabad ----------- -----------
2)Dr. Anil Kumar
Address of Applicant :Professor, Department of Electrical Engineering, SET, IFTM University Moradabad, UP 244001 Moradabad ----------- -----------
3)Mr. Ankur Chahal
Address of Applicant :Assistant Professor, Department of Electronics and Commnication Engineering, SET, IFTM University Moradabad, UP 244001 Moradabad ----------- -----------
4)Dr.Rahul Kumar Mishra
Address of Applicant :Director, School of Computer Science & Applications, IFTM University Moradabad, UP 244001 Moradabad ----------- -----------

(57) Abstract :
The present invention relates to the field of the energy aware security technique that can weed out misbehaving nodes from the network. The invention more particularly relates to the trust aware intrusion detection system based on cluster. Mobile Ad hoc Networks (MANET) has gained substantial research interest, owing to its easy deployment and inexpensiveness. However, the security of the network is the major concern, because of the absence of the central authority. This work addresses these issues by incorporating the trust mechanism in the cluster formation and routing. The chief node is selected on the basis of four trust parameters such as energy, packet delivery ratio, neighbour count and mobility. The chief node kicks off the misbehaving nodes during the process of routing. The proposed work is proved to be resilient against replay and sybil attacks.

No. of Pages : 29 No. of Claims : 7