Cluster Comput
DOI 10.1007/s10586-017-0927-z

Multi-level trust based intelligence intrusion detection system to detect the malicious nodes using elliptic curve cryptography in MANET

Opinder Singh[1] · **Jatinder Singh**[1] · **Ravinder Singh**[1]

Received: 30 January 2017 / Revised: 2 May 2017 / Accepted: 12 May 2017

Abstract Mobile ad hoc networks (MANETs) are qualified by multi-hop wireless links and resource restrained nodes. Generally, mobile ad hoc networks (MANETs) are susceptible to various attacks like gray hole attack, black hole attack, selective packet dropping attack, Sybil attack, and flooding attack. Therefore, the wireless network should be protected using encryption, firewalls, detection schemes to identify the attackers and decreasing their impact on the network. So, it's an essential task to design the intelligent intrusion detection system. This research work deals with designing the multi-level trust based intelligence intrusion detection system with cryptography schemes for detecting the attackers. In order to identify the attackers, we propose a novel trust management with elliptic curve cryptography (ECC) algorithm. At first, a trust manager is maintained, its functions is to classify the trust into three different sets of trust level based upon the elliptic curve cryptography and Schnorr's signature in the MANET. Each trust level has identified a single attacker. Thus, the proposed method has detected three types of attackers such as black hole attack, flooding attack and selective packet dropping attack. Furthermore, it have provided countermeasure for these attackers in the MANET as well as improved performances. Hence, it obtains higher throughput, minimum delay, minimum packet loss and efficient end to end delivery in MANET. Thus, the proposed scheme is a secure and optimal solution to encounter attackers, which represents to be efficient and significant.

✉ Opinder Singh
opindermca2008@gmail.com

Jatinder Singh
bal_jatinder@rediffmail.com

Ravinder Singh
dr.rs.global@gmail.com

[1] IKG PTU, Kapurthala, Punjab, India

Keywords Multilevel trust based intelligent intrusion detection system · Mobile ad hoc networks (MANETs) · Trust management · Elliptic curve cryptography (ECC) algorithm and malicious node

1 Introduction

MANETs have different aspects like security, IP addressing, routing, multiple access, service for handling wireless network communications. Network security is one of the major concerns in deploying the MANET applications, and thus, it gains interest among the researchers. In this section, the most important analysis is carried out in designing the secure framework, which would prevent the network from the attackers. Generally, MANETs are vulnerable in the operational functionality [1]; Interlopers can compromise the network activities by attacking any part of the network layers and Physical MAC; particularly, it affects network layer because of its poor routing algorithms, low-level batteries of the nodes, limited computational capacity of the nodes and undefined physical network location and short time nature of services in the wireless network [2]. Moreover, criterion followed for the measures of information security such as cryptography and key management scheme, have not given entire protection to the network [3]. Therefore, IDPS (intrusion and prevention system) are largely utilized to enhance the MANET security.

An IDS is a combination of software and physical components, which highlights the system activities in order to identify undesirable activities and issues (Fig. 1). For example, illicit and destructive activity, that captures the activities of security policy failure and also identifies dissatisfactory level in the security mechanism [4]. IDS are mainly used for securing the network organization systems. The volatile

Published online: 27 May 2017

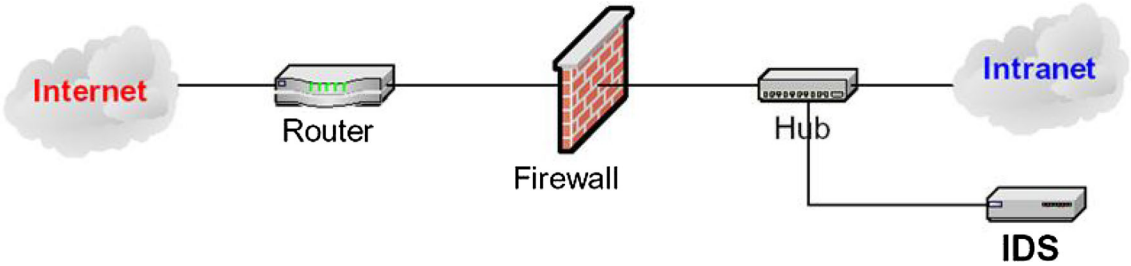

Fig. 1 A typical security scenario in any network [2]

development of the network frameworks can make the data exchange between the networks and computer, which is very crucial issues in the developing networking technology [5]. Meanwhile, it is a very difficult task to identify the attacker in the network which becomes hazardous in the network security, so, it needs to establish the proper procedure or protocol for security [6].

Intrusion generally refers to system attackers, which is causing vulnerable to various services such as hacking the information on the applications layer, host-based attack leads to login unapproved data or sensitive data that turns to be malware, viruses, worms and Trojan horses [7]. These types of attackers try to affect the confidentiality, integrity and accessibility of resources. Intrusions can also deny the administration's activities, system network by neglecting responses to without reveal about the information being stolen or lost. Intrusion detection systems used for identifying unapproved resource utilization of a system and also discovers attackers on a system framework or networks. IDS are implemented in software programming or hardware for identifying these kinds of attacks actions in the networks [8]. The previous network security framework considered firewalls, but it would not handle various network attackers on the application layer. For example, Black hole, packet drop attack DoS, DDOS attacks, worms, viruses, and Trojans. Besides the development of the Internet, the high prevalence of the attackers has causes for the major security concerns to consider IDSs [9].

In this paper, we propose an intelligent intrusion detection system (IIDS) with trust management and attackers detection algorithm for detecting the malicious nodes. We focus on detecting the attacks such as a black hole attack, selective packet dropping attack and flooding attack by using IIDS. Thus, the proposed scheme aims to generate the secure path to the nodes instead of shortest paths. Moreover, it produces all possible paths with their trust length; the highest trust length path is selected as a secure and best route for the routing process under AODV the routing protocols. Each level of trust identifies the sorts of attacks using proposed schemes. It aims to detect three different types of attackers, trust length ratio and improves the packet delivery ratio and throughput after the detection of the malicious node.

2 Literature review

Bace et al. [10], had proposed that host-based IDS. It aimed at collection and examination of data on particular host or framework. This host agent has used the supervised methodology for identifying intruders to trade off the system security techniques. HIDS plays various roles for antivirus. Therefore, antivirus should supervise all the network actions taking place inside the framework; however, it does not consider about buffer overflow assaults on system memory or malignant behavior of the operating framework function. Still, HIDS has verified and collected the system information including file system management, network events, and system calls to confirm whether any irregularity has happened or not. HIDS framework depends on vigorous on audit trail and network for identifying strange action inside the framework. The host-based framework had monitored the network to access the user particular information, which is a major reward [3]. HIDS had detected the unconventional user of management resources. By identifying assaults using the standard form (like past assaults or indicative of an assault), activities with that network had been ceased by subsequently stopping the assault. This was enormously valuable in frameworks where framework resources were accessed remotely in a standard way. Some major drawbacks as follows: (1) they can't view the system activity [3], (2) HIDS depend intensely on audit trails which had depleted numerous resources and space in the server and (3) deficiency of cross-platform interoperability.

According to Richard et al. [11], Snort, an open source network intrusion prevention system was introduced. It outperformed for performing the traffic examination and packet signing on IP systems. It dealt with different IDS approaches like buffer overflow, protocol evaluation, CGI assault and numerous attacks. Hence, they had reviewed the most common features of the network and host based system for IDS that detected the attacker's strategies and its characteristics and listed out the important characteristics of both host and network based IDS [9].

According to Kozushko et al. [12], Host based IDS has important functions on individual hosts/devices on the com-

puter network. It has monitored the inward and outward packets from the devices and generates warning signals to the administrator for identifying the suspicious movement in the system. System programming is utilized to diagnose the effect of assaults. An HIDS has required to be added on every machine and particular configuration to that software and operating system framework. HIDS has two main demerits. Firstly, identifying the activities, that consumes the highest amount of time and space. The second demerit was mainly for supervising an expansive and bigger system that required several sensors. These were the major drawbacks in host-based intrusion detection.

According to Abraham et al. [13], "SCIDS 2004 has aimed at IDS for analyzing and detecting the attackers using fuzzy rule based classifiers. Fuzzy had been considered for the application side of the fuzzy set hypothesis in order to manage the nodes performances with complex problems. By reviewing the paper, data is mined with ordinary information which has been contrasted with recognizing of attackers, so it was found that the detection accuracy has to be improved.

Toosi et al. [14] has demonstrated a method to detect the ordinary and unusual activities in the system by proposing adaptive neuro-fuzzy inference framework. It classified the typical and suspicious activities and identified the attackers. The IDS framework's main objective was to categorize of a framework into two major classifications: ordinary and suspicious (intrusion) performances. IDS frameworks can typically identify the several types of assault or group actions in some particular gatherings. The target of their methodology was to combine a few soft computing methodologies into the ordered framework to distinguish and categorized intrusions from typical activities performed on the computer network. At last, in order to accomplish the best result, genetic algorithm upgraded the structure of their fuzzy decision methodology. The examinations and performance of the proposed strategy were executed using the KDD Cup 99 intrusion detection dataset.

Abraham et al. [15] and Hubballi et al. [16] have proposed distributed IDS to identify interruption in a system. Their methodology was performed by using three fuzzy principles which were based on classifiers in a network to distinguish intrusion detection. Their methodology, particularly concentrated on helpful IDS operators for investigating the intruder's assault methodologies, which helps in distinguishing local event examination to understand the attacker's strategy. Moreover, system investigation has provided a chance for IDS operators to pro-actively look ahead for information which is correlated to current case advancement. Their methodologies have concentrated on defined framework with maximum resources for gathering and examining those events which were destined to expose intrusions.

Wang et al. [17] has analyzed about the trust derivation values and their related evidences. The resources of the network node are performed periodically. The reputation and trust value are inter exchanged depend on the intrusion detection technique and which provides the variations in the trust value.

Gonzalez et al. [18] has introduced a new algorithm that describe about the basic flow of accusation and conservation of nodes for discovering misbehavior node. Based on the threshold value, it can classify the misbehaved and normal nodes in the network. However, it fails to improve the performance of the system which cannot obtain the average data transmission ration in the network.

Nadeem et al. [19] has proposed Hierarchical based IDS for DoS attack in MANET. They have utilized adaptive intrusion detection and prevention (AIDP) technique to distinguish DoS assaults created by malicious RREQ flooding in MANET. AIDP comprises of training module and testing module. They separate the system into bunches then select the most proficient hubs as cluster head (CH) and remaining hubs as cluster nodes (CN). CH ceaselessly gathers data in the preparation module and produces an underlying preparing profile (ITP). In the testing module the CH has the duty to distinguish the interrupting hubs and disconnect these nodes by advising all CNs.

Zhexiong et al. [20] proposed a unified trust management scheme that improved the MANET security. Utilizing late advances as a part of questionable thinking, Bayesian derivation, and DST, we assess the trust estimations of watched hubs in MANETs. Mischievous activities, for example, dropping or altering data can be recognized in our plan through trust values by immediate and backhanded perception. Nodes with low trust qualities will be avoided by the directing calculation. In this manner, a secured path can be set up in insecure situations. More exact trust was acquired by considering diverse sorts of packets, indirect perception from hop nodes, and others nodes lines and conditions of remote associations, which may bring about packet loss in neighbor nodes.

Suparna et al. [21] has discussed about the black-hole attack and introduced a solution depend on trust values of the single node to identify and prevent the system from the black-hole attack in MANET, which assures secure packet transmission along with significant resource usage of mobile hosts at the same time. Trust has been estimated depend on the certain essential parameters of a node such as battery power, rank and mobility, etc. The performance analysis of trust of each node in the network is depend on parameters such as node stability was determined by its mobility, reliability and pause time, rest of the battery power etc. This trust value of a node makes the selection of the best reliable route for data transmission. The experimental results have demonstrated that the proposed method gives better performance in terms of secure routing of data, throughput and significant resource usage.

2.1 Challenges

There are numerous challenges in designing IDS for MANETs. First and foremost challenge is designing IDS to make sure that all the elements are considered to detect the intrusion. The choice of an appropriate set of features would provide perceptivity into the basic network performance which is available in the audit data and ultimately improve the overall accuracy in the IDS. To detect the intrusion with the particular time period is a major concern in the IDS. It is essential to detect and remove the intrusion from the system quickly, as it could damage the system [22]. Therefore, it should be prevented and recovered in a rapid manner. Next, the challenge was detecting the intrusions quickly or else the system performance would lead to degraded. Then, the upcoming challenge is selecting the exact method to identify the intrusions by means of selecting the precise algorithm for detecting misuse and anomaly methods with various considerations of different parameters to detect the intrusions. Anomaly detection systems are also hard to train in highly dynamic environments. The most important challenge was to develop the intrusion detection with response system while holding the preferred network performance, so there is a huge demand to design the framework for IDS. It is essential to design the IDS more effective in detecting the various type attackers with fewer false positive. Additionally, it has to maintain the size, speed and dynamic networks in MANET.

3 Research methodology

In this research, we design the framework of the multilevel based intelligence intrusion detection system which can handle various types of attackers like black hole attackers, flooding attackers and selective packet dropping attackers. The proposed architecture diagram is represented in Fig. 2. The proposed scheme deals with the multilevel based trust with elliptic curve cryptography that can estimate the type of attackers going to affect the system security and also prevent the system from the attackers. We propose multilevel intelligence intrusion detection system, which makes use of trust mechanism along with cryptography schemes. The research methodology consists of the few techniques which are combined with trust based elliptic curve cryptography in order to detect the flooding attack, black hole attack and selective packet dropping attack, therefore, it is termed as multilevel intelligence intrusion detection system. These attackers are detected under the modified AODV protocol. It provides the detailed description of the trust management approach and its trust elements in the below section.

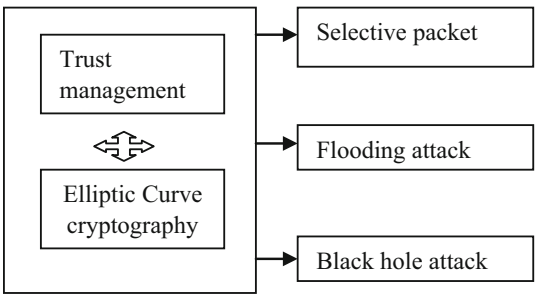

Fig. 2 Block diagram—proposed methodology

3.1 System model

In our proposed system, we consider an intelligence intrusion detection system in the Mobile Ad hoc system with dimensional trust elements in order to obtain the multi-level trust value, by transmitting the data from source to destination. The trustworthiness of the nodes is estimated from the following dimensional trust factors:

1. Direct trust
   1.1 Auto trust
2. Indirect trust
   2.1 Other's trust
3. Subject trust
4. Objective trust
5. Static trust
6. Dynamic trust

The trust element of the nodes in our model, is described in six groups of trust level, as mentioned above, actually, it classified into three sets of groups, the first set has direct and indirect trust that support trust for node's movements and it is further classified into auto and others trust. Second set of trust is defined as subjective and objective trust; it is used for key authentication and authorization values. Finally, the third set of trust group, static and dynamic, is estimated by the symmetric and asymmetric value of the key generation. In our proposed system, we estimate the trust value by considering the following conditions in the Trust management approach in the MANET.

3.1.1 Trust management approach

In this model, trust manager maintains the trust value of all its nearby nodes through the three sets of trust levels. The direct trust value is estimated using the auto trust in which the nodes gains the trust by the amount of the packet delivered without any delay. Indirect trust value is estimated through the Other's trust value which means that the reputation of the node. Subjective trust is determined by the node trust value for component X is estimated by the node aggression of the

Table 1 Notation

Symbols	Description
n_j	Sink node
n_i	Number of nodes acts respondents in the network for data packet transmission
n_{nb}	Number of neighborhood nodes in the network
SID_i	Secret key identifier for the asymmetric key of node n_i to n_j
UID_i	Unique key identifier for the symmetric key of the node n_i
W_{ij}	Witness produced by the node n_i to n_j
$Trust_{FS}$	It presents first set of trust level for direct and indirect trust value within the range of [0,1]
$Trust_{SS}$	It presents second set of trust level for objective and subjective trust value within the range of [0,1]
$Trust_{TS}$	It presents third set of trust level for static and dynamic trust value within the range of [0,1]
$E(F_p)$	Elliptic curve over a finite field of F_p
ρ	A constant normalize for the competence
α	The weight with direct evidence in attack behavior
$DLOG$	Discrete logarithm problem in elliptic curve
$[X] \times P$	Elliptic curve scalar multiplication over F_P with the base point P
$\|\|$	Concatenation operator
TL	Trust length
H(.)	Hash function value
NTT	Neighbor trust table
OTC	Overall trust value along cryptography

Direct and Indirect trust of the node in the network along with key authenticity value, in case the node agrees the node key as an authentic, only when the key is generated as the secret key to the particular node that has generated the witness. In objective trust, it recommends for the nodes, nodes obtains its recommendation based on the witness of the key authorization of the nodes, it can derive the trustworthiness value. The static trust is determined by the key generation of the symmetric key value from the one node to another node, and the dynamic trust is estimated by the asymmetric key value from one node to the sink node. Based on all the trust values, it estimates the overall trust value of the network along the cryptography techniques. In case the node is repeatedly utilized for data transmission, then it would have trust value and risk of getting affected by malicious nodes. Hence, the risk level will be very low, while comparing the other normal node.

In the node deployment, the proposed scheme consists of the three stages, the registration stage, login stage and authentication stage. In this section, it describes about the node organizer for deploying the sensor node and sink node in the mobile ad hoc network and all the stages. The notations are illustrated in Table 1. MANET requires the pre-deployed phase for enabling the nodes in the networks. Here, the node organizer plays an important role in managing the node performance. Each constrained node in the IDS is predetermined. In the proposed intrusion detection system, the steps are as follows:

- Trust level from the neighbor node is indicated as a node n_{nb}, the nearby nodes of n_0, is a group of nodes by having one hop contact with node n_0 and are demonstrated as $N_{nb}(n_0) = \{n_1.....n_n\}$.
- If observer node n_i is selected from the set of nodes in $S_{ni} = \{S_1.....S_n\}$. The action of the node n_i is monitored by another node n_0 by monitoring its individual activity.
- The monitored activities of node n_i are stored by the dimensional vector d $n_i = \{d_1 n_i.....d_s n_i\}$ with every factor which demonstrated about the node's actions in a single feature.
- In case node n_i monitors its nearby nodes $N_{nb}(n_0) = \{n_1.....n_n\}$, it stores set of the matching attribute vectors $SN_{nb}(n_0) = \{S_{n1}.....S_{nn}\}$, the trust value of the sink node is estimated as n_j using our classified trust level.

3.2 Multi leveltrust based ECC cryptography

Elliptic curve cryptography is another solution for the public key cryptography. It depends upon the algebraic calculation of elliptic curves over finite points. It considers p as a prime number and F_p as finite field. Generally, elliptic curve E is determined as a nonsingular curve, i.e. given as: $Y^2 = x^3 + ax + b$, where a,$b \in F_p$ are defined as arbitrary constants which meeting the $4a^3 + 27b^2 \neq 0$. A pair of (x, y), where x, $y \in F_p$, is specific points on the cure that can meet the requirement of the above equation. Hence, the elliptic curve points of (x_1, y_1) and (x_2, y_2) are used for the point addition in order to generate the third point in the curve. The elliptic group theory contains the group operation performances with a set of points (x_2, y_2) to the actual point of the curve in making the Abelian group with the center point O represents as identity element. Therefore, the elliptic curve forms certain special features that prepare themselves essential for security applications. The p is defined as the prime number in the field where f is defined as the binary case. The cyclic subgroup of $E(F_p)$ is determined by its key generator P and order n, it is called as base point.The public domain parameters considered in the elliptic curve are p as the prime and a, b are determined as constants and order n in the field points. The secret private key is randomly selected from the integer s with uniformly in the range of $[1, n]$, whereas the corresponding public key is estimated by $Q = [s] \times P$. In discrete logarithm problem, it is very essential to make use of an ECC mechanism in order to improve the double point scalar multiplication.

The proposed feature in this method is to highlight that each node has public and private key for encrypting and decrypting the data in the network. Each noden_i, has its secret private key SID_i through its corresponding public key UID_i can authenticate the data without demanding for any certificate from the third party, hence, we define as self- certified symmetric key approach. Our proposed algorithm benefits the advents of ECC and Schnorr's signature.

The recommendations of the nodes are combined as a set of the node's symmetric and asymmetric key. In our proposed model, we have certain assumptions of generating the secret key generation within the proposed trust management approach. At the beginning, the respondents nodes n_i accept on the ECC Schnorr's set up parameters such as ($E(F_p)$, n, P, H) is discussed in the above section. The secret key generation with equating the public key of the node, it is represented as

$$SID_i = UID_i \times 2P \tag{1}$$

Every node in the network has its own attributes (ID_i;SID_i; UID_i) which meets a computationally reliable relationship that is confirmed implicitly by the efficient usage of the secret key (SID_i) in any cryptographic operation. We utilize three sets of the levels of the trust value, defined as multi-level trust value. Hence, the trust value of nodes from node n_i to n_j sink nodes are represented by the trust component X's (First set level of trust, Second set level of trust and Third set level of trust) along with the time t duration and the notations are represented as $T_{i,j}^{I,D}(t)$, $T_{i,j}^{S,O}(t)$, $T_{i,j}^{S,D}(t)$.

3.2.1 Algorithm

(a) Set up:

At first initialize (UID_i/SID_i) as the signer's Public key identifier/ secret private key identifier, where the public key is selected using a pseudo random number generator from [1,n] and the secret private key is selected as $SID_i = UID_i \times 2P$

Choose the hash function in the range of $H : \{0, 1\}^* \rightarrow [1, n]$

(b) Witness extraction:

To create the witness on theID_i, it requires the trustee node n_i to generate the witness for the n_j as follows:

n_i selects the random integer from the range $K_{ij} \in [1, n]$ and it estimates the recommendation value from the R_{ij}

$$\bar{R}_{ij} = K_{ij} \times P \tag{2}$$

where K_{ij} represents to authentic node n_i to n_j sink n_i calculates for the $\bar{R_{ji}}$, recommendation value from the sink node n_j to n_i node

$$\bar{R}_{ji} = \sum_{n_i \in Trustee} \bar{R}_{ji} + [a_j] \times P \tag{3}$$

where a_j is secret random number from$[1, n]$. n_i calculates for the overall recommendation value as

$$R_{ij} = \bar{R}_{ij} + \bar{R}_{ji} \tag{4}$$

$$n_i \text{ Calculates for } h_{ij} = H(ID_{ij}||R_{ij}||T_{val}||Rec_{ij}) \tag{5}$$

where T_{val} represents the trustee value from the node n_i to n_j sink.

Which h_{ij} describes the concatenation of all recommendations value from the all the trust level of the nodes issues from the n_j sink node, the witness is extracted as

$$W_{ij} = SID_i.h_{ij} + K_{ij} \bmod (n) \tag{6}$$

(c) Secret key generation

The secret key is generated finally as

$$SID_{ij} = \sum_{n_i \in Trustee} W_{ij} + a_j \bmod (n) \tag{7}$$

(d) Self-certified for public and private key generation

Here, it first uses the symmetric key and asymmetric key generation, public key verification for one to another node and the Public key exchange (asymmetric key) for node to sink authentic as well as vice versa

$$PK_A = PK_{SA}^{h(ID_A||R)}.R(\bmod p) \tag{8}$$

3.3 First level of trust

3.3.1 Direct trust value

When the node is ready for the data transmission, At first we consider that a node has its individual trust profile is present, depicting its inherent behavior patterns that would present within the range of [0, 1]. The direct trust value of a node depends on the difference between actual time and estimated time to complete process along with the witness value. The node obtains the witness value is based on the node n_i accepts to public key and authentic with the sink node n_j, hence it produces the witness value to improve its trust value By the difference between the actual time and the estimated, finally

approximate time of the node is obtained in order to get the direct trust value of the node.

$$\text{Direct trust value} = T_{DT} = (T_i^X) - (A_i^X - E_i^X) + W_d) + T_{AT} \tag{9}$$

where the auto trust value is generated, it directly associated with direct trust value, it is given as

$$T_{AT} = \frac{1}{T_{DT}} \tag{10}$$

3.3.2 Indirect trust value

The Indirect trust value of the node is estimated, when the node agrees to authentic the public key of another node, which does not have the witness value, and moreover, it is authenticated by the node n_j. Hence, the indirect trust value will not have the recommendation for the other's nodes. But, it has obtained the trustworthiness of the nodes later on, whereas, the other trust value is determined, it directly associated with indirect trust value, it is given as:

$$T_{OT} = \frac{1}{T_{ID}} \tag{11}$$

$$\text{Indirect trust value } = T_{ID} = (T_i^X) - (A_i^X - E_i^X) + T_{OT} \tag{12}$$

$$Trust_{FS} = T_{DT} + T_{ID} \tag{13}$$

Neither direct trust nor the indirect trust value is reduced due the time duration for the authentic and acknowledgement from the sink node, it automatically fails to authentic or delayed that leads to highest risk of flooding attack.

3.4 Second level of trust

3.4.1 Objective trust

We consider the node's trust profile is available, in which objective trusts depend upon the competence level which includes energy reduction, link failure and involuntary or voluntary network disconnections. This is estimated by the ratio of the packet forwarding in the networks. In multi hop conditions, a node sends the packet to its nearby nodes. The ratio of the packet is obtained by a node and their later sending node to its target node is referred as Packet Forwarding Ratio. PF_c is the packet forwarding ratio of node n observed by the node n_0. A node is considered to be affected selective attack only if its packets forwarding ratio is much meager than the packets forwarding ratio of its nearby nodes. The trust value of the node is determined by these groups of attributes such as energy reduction, link failure and involuntary or voluntary network disconnections.

$$\text{Objective trust value } T_{OT} = \rho P_i^c(t) \times PF_c + P_r \tag{14}$$

3.4.2 Subjective trust

In the subjective trust calculation, it involves as node trust value for component X is estimated by the node aggression of the direct and indirect the node in the network along with key authenticity value with acknowledgement of the sink node including its function at its time duration. Therefore, it is estimated in terms of packet receiving ratio PR_c in the components X in the network.

$$\text{Subjective trust value } T_{ST} = \alpha T_{DT}^{i,j}(t) + (1-\alpha) T_{ID}^{i,j} + PR_c \tag{15}$$

$$Trust_{SS} = T_{OT} + T_{ST} \tag{16}$$

Neither objective nor the subjective trust value is reduced due the time duration for packet forwarding ratio and packet receiving ratio that leads to highest risk of getting selective packet dropping attack.

3.5 Third level of trust

3.5.1 Static trust

The final set of trust deals with two categories like static and dynamic trust value. The static trust value is evaluated by the symmetric key from the node n_i to n_j sink node, here, it analysis, whether all the packets have sent the packet transmission request to other nodes with a symmetric key, where it utilize the node capacity level and it maintains the historical trust level of the each node separately in the trust table, as it consider the time duration of the request of the route. The trust table continuously analyzes the node's trust value and it updates the trust value of the entire node in the table. The node capacity level for achieving the packet transmission services at time t, which considers the ratio of battery, bandwidth, CPU cycle, route request and the memory at that point. The static trust value is represented in the form of the equation, which is given below

$$T_{ST} = N_c(t) + TV(t) + CPF_i + K_{sym} \tag{17}$$

3.5.2 Dynamic trust

For the dynamic trust estimation, it analyzes the asymmetric key for the key generation and the verification, as same as the static value process, but, it includes the witness extraction

Table 2 Attacker detection and prevention

Attack behavior	Detection	Countermeasure
Flooding attack	The first order trust value of direct and indirect value are used to estimates the time duration for the authentic and acknowledgement from the sink node n_j to n_i, which fails to authentic or delayed, identified as flooding attack	large time taken is to authentic and acknowledgement from the sink node n_j to n_i, it detects specific nodes with delay ack are given no recommendation value, it is updated in the trust table
Select packet dropping	The lower second level of trust value, it associates with the packet forwarded ratio and packet receiving ratio	After the overall trust value updating in the table, it eliminates the existing routing path and recommendation value of each node will be varied
Black hole attack	If it has the higher difference in the route quest and the route reply is detected as black hole attack which is due to the minimum trust value in third trust level	Once, after the updated trust value, the only secure routing path is used for routing, therefore there will n ot be higher difference in the route request and route reply

value that varies with control data packet, and the data forwarding packet as well as the time duration of the response of the route in the dynamic trust value estimation.

$$T_{DT} = N_c(t) + TV(t) + W_1 \times CPF_i + W_2 \times PF_c + K_{asym} \tag{18}$$

$$Trust_{TS} = T_{ST} + T_{DT} \tag{19}$$

Neither static nor the dynamic trust value is reduced due the time duration for packet route requests and routeresponse that leads to higher risk of getting black hole attack.

There are three ways of estimating about the monitored node that means, a node may be considered as secure or it can be considered as risky node or a suspicious node. These node's information is stored and send through the forwarding engine to the central network administrator for secured IDS. Trust value is estimated by the following trust like as direct trust, auto trust, indirect trust, others trust, subjective trust, objective trust, static trust and dynamic trust. Thus the overall Trust value is given as:

$$\text{OTC} = (Trust_{FS} + Trust_{SS} + Trust_{TS}) \tag{20}$$

The anti black hole mechanism is, ultimately, utilized to identify the secure routing path between source and destination by verifying the check messages. Later on the detection of the black hole node and the suspicious node ID is included in the block table, it is represented in Table 4, in order to forward BLOCK message for the entire network to isolate the suspicious node. When a route request (RREQ) is received from a node during which it estimates the static value of the trust, it would verify whether that is arriving from the block table, if it identifies that the node id is present in the table, source node would remove the RREP; or else the source node saves the (route reply) using the dynamic trust value in RREP table and then the performance is continuously exceeded until the time ends, it is termed as 'anti black hole mechanism'. Thus, we would prevent the black hole problem in the MANET. The proposed intrusion detection system nodes would undergo anti block hole mechanism, which is importantly used to determine the malicious node by using an amount of a huge difference between the RREQs and RREPs data transmitted from the node.

In this intrusion detection system, we have proposed detecting the malicious node algorithm which detects the attackers under the AODV routing protocol. The data packets are carried in the AODV-MAC layer, while a node wants to perform the channel. Each intermediate node is:

1. At first, it initializes the node n, source node n_s, destination, neighbor node n_0 and monitor node n_i under the AODV protocol. It includes nearby nodes in the one hop count is given as $N_{nb}(n_0) = \{n_1 \ldots\ldots n_n\}$, node's attributes as $S_{ni} = \{S_1 \ldots\ldots S_n\}$and dimensional vector d, $n_i = \{d_1 n_i \ldots\ldots d_s n_i\}$.
2. Next, the trust manager is incorporated in the multi-level based intelligence intrusion detection system, which gives the trust value to the nodes depend on the as direct trust, auto trust, indirect trust, others trust, subjective trust, objective trust, static trust and dynamic trust with ECC. The overall trust value should be equal or greater than the trust value with cryptography (OTC) and the trust value calculation is given

   $$OTC = (Trust_{FS} + Trust_{SS} + Trust_{TS})$$

3. The node n_i observes the activities of the nearby nodes that estimates whether the node is a secure node or risky node or malicious node nodes. It classifies the node's

Table 3 Simulation parameters

Stimulation	Parameters
Simulation area	800 m × 800 m
Simulation time	60 s
Number of nodes	100 N
MAC layer	IEEE 802.11
Transmission range	250 m
Packet size	512 bytes
Traffic pattern	CBR (constant byte rate)

behavior node by using the behavior classifier using multilevel trust based ECC as per their activities in the MANET.

4. Then, the detection of malicious node or the attackers is identified with the help of risk factor calculation, trust value of static and dynamic and finally by estimating the abnormal amount of difference between the RREQs and RREPs through anti-black hole mechanism.
5. Then the antihole mechanism is adopted, it detects the suspicious node by using the amount of huge difference between the RREQs and RREPs data transmitted from the node.

Thus, the proposed detection of malicious node algorithm is capable of identifying the flooding attackers, selective packet dropping and black hole attackers and prevents the network from these attackers; it is presented in Table 2. The identified attackers are moved by the forward engine to the central network administrator, in which central network administrator will not forward the data packet through the malicious nodes and eliminates malicious node from the network. The conditions for forwarding the data are a selection of the secure routing path instead of the shortest path.

3.6 Case conditions

Case 1 In this case, trust value with cryptography (OTC) is estimated as OTC= $(Trust_{FS} + Trust_{SS} + Trust_{TS})$ and as $Trust_{FS} = T_{DT} + T_{ID}$ is lesser than Second level of trust value and Third level of Trust value, i.e. neither $T_{DT} = 0$ nor $T_{ID} = 0$ or when both remain to be zero, then it becomes $(0 \leq Trust_{FS} \leq Trust_{SS} + Trust_{TS})$. Then, it is identified that, it has the risk of attacked by the Flooding attack.

Case 2 In this case, trust value with cryptography (OTC) is estimated as OTC= $(Trust_{FS} + Trust_{SS} + Trust_{TS})$ and as $Trust_{SS} = T_{OT} + T_{ST}$ is lesser than First level of trust value and Third level of Trust value, i.e. neither $T_{OT} = 0$ nor $T_{ST} = 0$ or when both remains to be zero, then it is becomes $(0 \leq Trust_{SS} \leq Trust_{FS} + Trust_{TS})$ Then, it is identified that, it has the risk of attacked by the selective packet dropping attack

Case 3 In this case, trust value with cryptography (OTC) is estimated as OTC= $(Trust_{FS} + Trust_{SS} + Trust_{TS})$ and as $Trust_{TS} = T_{ST} + T_{DT}$ is lesser than First level of trust value and second level of Trust value, i.e. neither $T_{ST} = 0$ nor $T_{DT} = 0$ or when both remains to be zero then it is becomes $(0 \leq Trust_{TS} \leq Trust_{FS} + Trust_{SS})$ Then, it is identified that, it has the risk of Black hole attack.

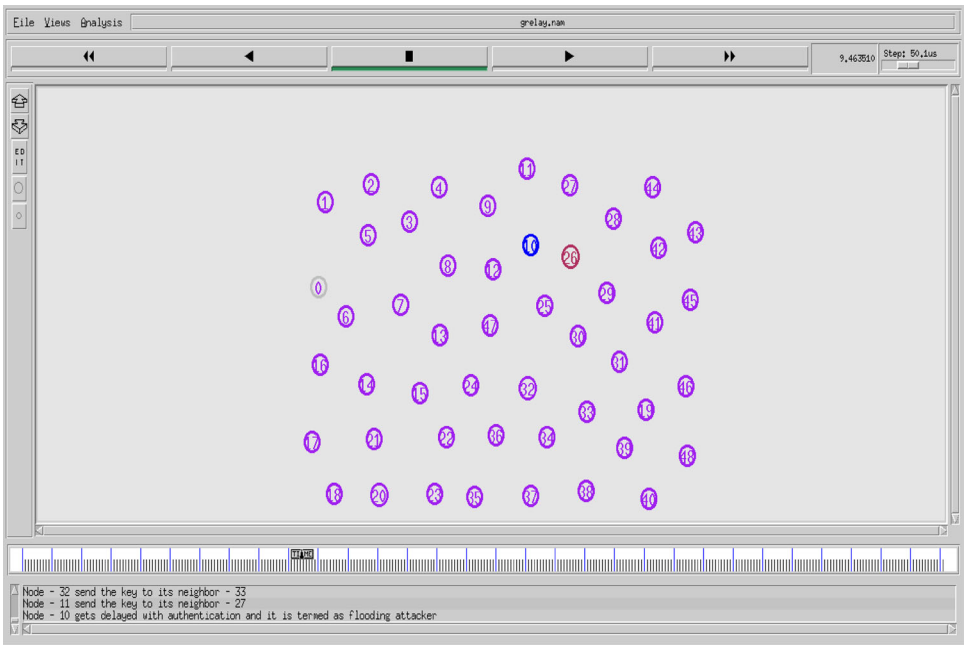

Fig. 3 Detection of the flooding attackers in MANET

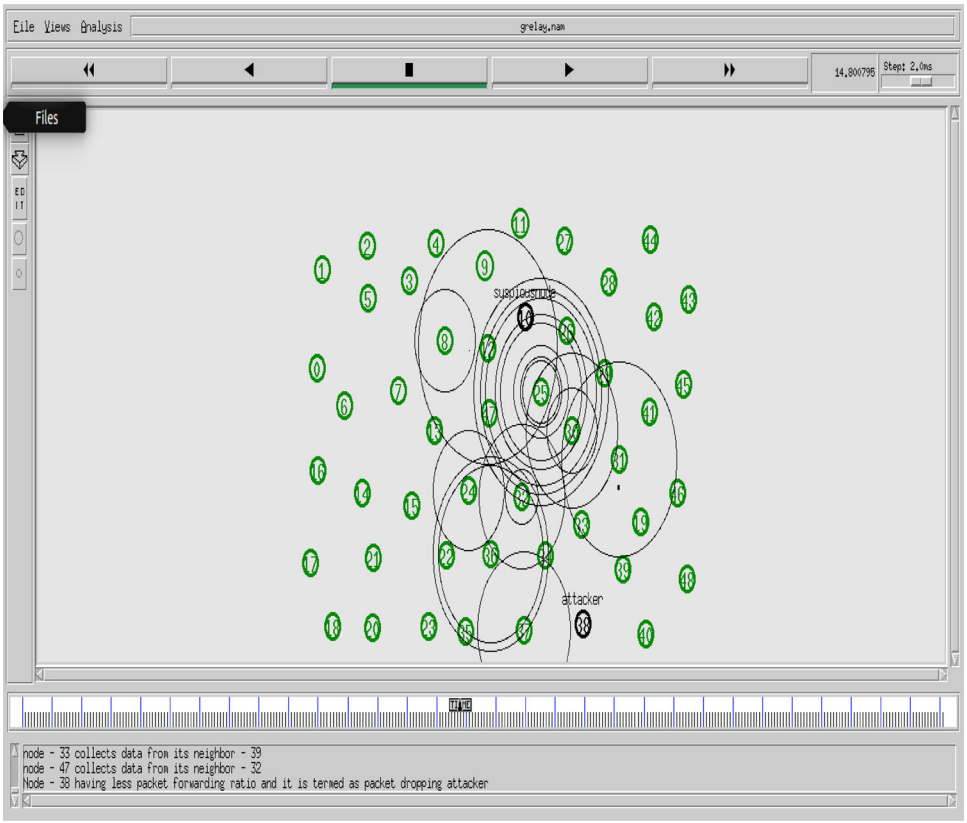

Fig. 4 Detection of the selective packet dropping attackers in MANET

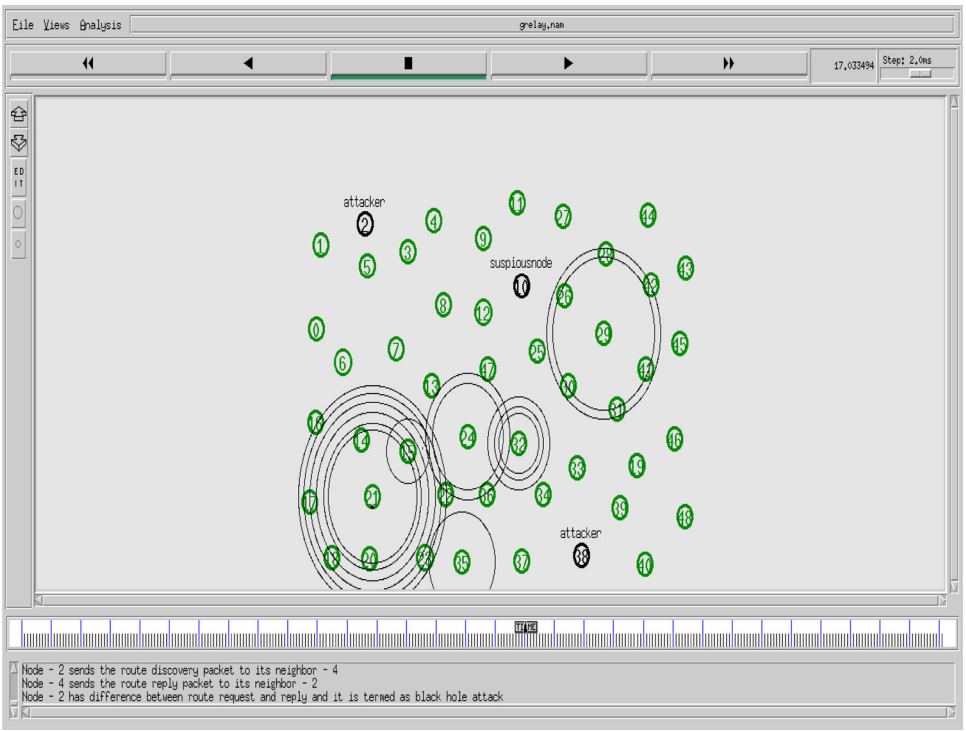

Fig. 5 Detection of the black hole attack in MANET

4 Performance analysis

The proposed model in the intrusion detection system is simulated in the NS2 network simulator version 2.33 (NS2.33) [23]. The 802.11 MAC layer is utilized for in *NS-2* simulation. The nodes are deployed randomly and the stimulation parameters are given below:

It has carried out the simulation with a maximum of 100 nodes that estimated the node speed versus routing packet rates, packet delivery ratio and the throughput of the network is calculated, stimulation parameters are mentioned in Table 3. The proposed model in intrusion detection system identifies all the attackers such as flooding attack, black hole attack and the selective packet dropping attackers. In Fig. 3 represents about the detection of flooding attack, Fig. 4 demonstrates about detection of selective packet dropping attack and Fig. 5 represents the black hole attack.

The proposed method detects three attacks using of malicious algorithm and protect the network from these attackers for the data transmission from the node through the difference between the RREQs and RREPs, it is estimated in Table 4

The node form the source to destination and their neighbor nodes are detected. The first level set of trust, second level of trust and third level of the test is determined in Table 5. Depend upon the trust length, it estimates the secure path for nodes in which the packets are delivered in the selected secure path by identifying the attacks. The trust length is evaluated with respective computational time and from the

Table 4 AODV parameters

Parameter	Value (s)	Parameter	Value
Active route T/O	12	RREP wait time	1S
Rev. route Life	7	#RREQ retries	2
Max.RREQ T/O	12	Link Layer Det.	Yes

Table 5 Trust length

First level of trust	Second level of trust	Third level of trust	Trust length
0	1	1	2
1	0.2	0	1.2
0.5	0	1	1.5
0	1	0.7	1.7
1	0.3	0	1.3
0.5	0	1	1.5
0	1	0.3	1.3
1	0	0.5	1.5
0	0.9	1	1.9
1	0	0.4	1.4
0.6	1	0	1.6

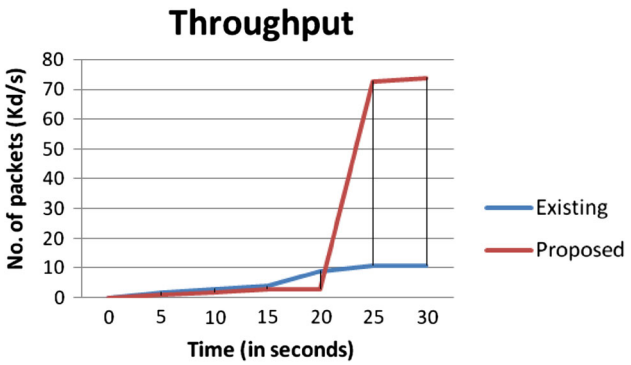

Fig. 6 Throughput

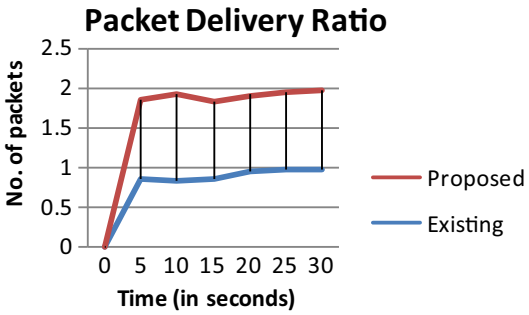

Fig. 7 Packet delivery ratio

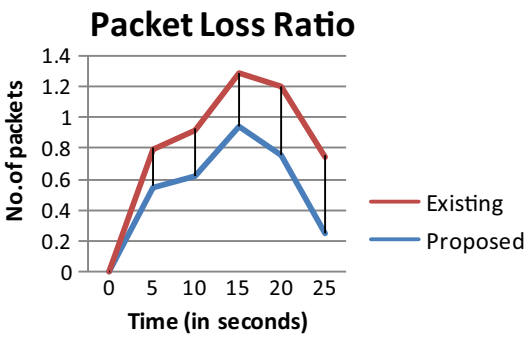

Fig. 8 Packet loss ratio

experimental outcome, it proves the proposed approach is more effective than an neighbor node trust method [24].

Hence, the throughput, packet delivery ratio, packet loss, delay and end to end delay are calculated to determine the performance of the method. Figures 6, 7, 8, 9 and 10 demonstrates about the performance metrics of the MANET. Thus the important metrics such as packet delivery ratio (PDR), throughput, packet loss, delay and packet overhead are observed, in which these results in Figs. 6, 7, 8, 9 and 10 have proved that the proposed system has effective than neighbor node trust method [24]. Therefore, the experimental results demonstrate the significance of the proposed methodology.

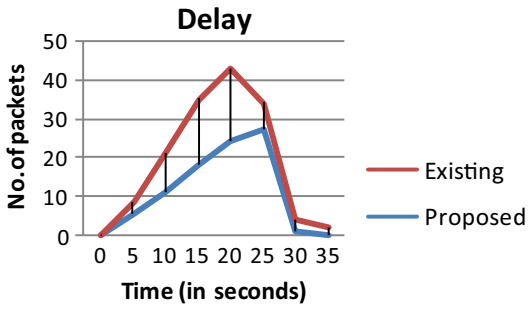

Fig. 9 Delay

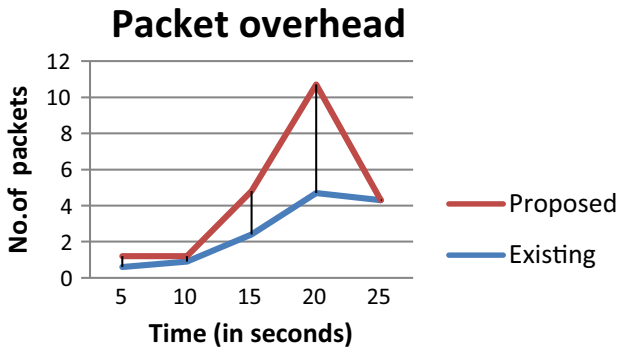

Fig. 10 Packet overhead

5 Conclusion

This research study has addressed the different security issues in designing an intrusion detection system in mobile ad hoc network (MANET). However, AODV protocol is susceptible to various attacks because of this weakest security design. We focus on detecting the attacks such as a black hole attack, flooding attack and selective packet dropping attack by designing multi-level trust based intelligence intrusion detection system with cryptography scheme. In this paper, we utilize the multi-level intelligent intrusion detection system for detecting the malicious node with the help of trust management and elliptic curve cryptography. In trust management based on the three levels of trusts such as level-1 are direct trust, auto trust, indirect trust, others trust, level-2 are subjective trust, objective trust and level-3 are static trust and dynamic trust, the proposed system estimates the trust length and key verification. If the trust length is maximum then risk factor is the minimum possibility of the attackers is remains to be zero or else the flooding and selective packet dropping attackers are detected through the ECC algorithm. Moreover, it produces all possible paths with their trust length and highest trust length path is selected as a secure and best route for the routing process under AODV. The antihole mechanism is adapted to detect the black hole attacker, by the amount of difference between the RREQs and RREPs is higher during data transmission. Hence, it eliminates malicious node from the network in order to obtain higher packet delivery ratio, throughput, minimum delay, minimum packet loss and efficient end to end delivery with high security in MANET. Thus, simulation results for detection of the black hole attacker, trust length ratio, and the performance metrics are effective in this strategy. Hence, the proposed method is more significant than the neighbor node trust method. In future enhancement, this mechanism would extend to identify lot more attackers in the MANET.

Acknowledgements Authors are highly thankful to the Department of RIC, IKG Punjab Technical University, Kapurthala, Punjab, India for providing the opportunity to conduct this research work.

Compliance with ethical standards

Conflict of interest The authors declare no conflict of interest.

References

1. Siva Ram Murthy, C., Manoj, B.S.: Ad Hoc Wireless Networks, Architecture, and Protocols. Prentice Hall PTR, Upper Saddle River (2004)
2. Basagni, S., Conti, M., Giordano, S., Stojmenovic, I.: Mobile Ad Hoc Networks. IEEE Press, Wiley (2003)
3. Aggelou, G., et al.: Mobile Ad Hoc Networks, 2nd edn. McGraw Hill Professional Engineering, Oxford (2004)
4. Chlamtac, I., Conti, M., Liu, J.J.-N.: Mobile ad hoc networking: imperatives and challenges. Elsevier Netw. Mag. **13**, 13–64 (2004)
5. Belding-Royer, E.M., Toh, C.K.: A review of current routing protocols for ad-hoc mobile wireless networks. IEEE Pers. Commun. Mag. **6**(2), 46–55 (1999)
6. Banerjee, S.: Detection/removal of cooperative black and gray hole attack in mobile ad-hoc networks. In: Proceedings of the World Congress on Engineering and Computer Science (2008)
7. Jain, S., Jain, M., Kandwal, H.: Advanced algorithm for detection and prevention of cooperative black and gray hole attacks in mobile ad hoc networks. J. Comput. Appl. **1**(7), 37–42 (2010)
8. Agrawal, P., Ghosh, R.K., Das, S.K.: Cooperative black and gray hole attacks in mobile ad hoc networks. In: Proceedings of the 2nd International Conference on Ubiquitous Information Management and Communication, pp. 310–314. Suwon, Korea (2008)
9. Baadache, A., Belmehdi, A.: Avoiding black hole and cooperative black hole attacks in wireless ad hoc networks. J. Comput. Sci. Inf. Secur. **7**(1), 10–16 (2010)
10. Bace, R., et al.: An Introduction to Intrusion Detection & Assessment. Infidel Inc., prepared for ICSA Inc. Copyright 1998 (1998)
11. Richard. M., et al.: Intrusion Detection FAQ: Are their limitations of Intrusion Signatures. http://www.sans.org/security-resources/idfaq/ limitations. PHP, April 5 (2001)
12. Kozushko, H.: Intrusion detection: host based and network-based intrusion detection systems. Indep. Study **11**, 1–23 (2003)
13. Abraham, A., et al.: SCIDS: a soft computing intrusion detection system. In: WDC 2004. LNCS, School of Computer Science and Engineering, Chung-Ang University, Korea, Springer, Berlin, Heidelberg, vol. 3326, pp. 252–257 (2004)
14. Toosi, A.N., Kahani, M.: A new approach to intrusion detection based on an evolutionary soft computing model using neuro-fuzzy classifiers. Comput. Commun. **30**(10), 2201–2212 (2005)

15. Abraham, A., Jain, R., Thomas, J., Han, S.Y.: D-SCIDS: distributed soft computing intrusion detection system. J. Netw. Comput. Appl. **30**(82), 81–98 (2007)
16. Hubballi, N., et al.: Fuzzy mega cluster based anomaly network intrusion detection, In: International Conference on Network and Service Security, 2009. N2S '09. ISBN: 978-2-9532-4431-1 (2009)
17. Wang, F., Chen, H., Zhao, J., Rong, C.: IDMTM: a novel intrusion detection mechanism based on trust model for ad hoc networks. In: 22nd International Conference on Advanced Information Networking and Applications, AINA 2008, pp. 978, 984
18. Gonzalez, O.F., Ansa, G., Howarth, M., Pavlou, G.: Detection and accusation of packet forwarding misbehavior in mobile ad-hoc networks. J. Internet Eng. **2**(1), 181–192 (2008)
19. Nadeem, A., Howarth, M.: Adaptive intrusion detection & prevention of denial of service attacks in MANETs. In: ACM, 2009 (2009)
20. Wei, Z., et al.: Security enhancements for mobile ad hoc networks with trust management using uncertain reasoning. IEEE Trans. Veh. Technol. **63**(9), 4647–4658 (2014)
21. Biwas, S., et al.: Trust based energy efficient detection and avoidance of black hole attack to ensure secure routing in MANET. In: Applications and Innovations in Mobile Computing (AIMoC), 2014 (2014)
22. Agarwal, U., Yadav, K.P., Tiwari, U.: Security threats in mobile ad hoc networks. Int. J. Res. Sci. Technol. **2**(2), 53–64 (2015)
23. Issariyakul, T., Hossain, E.: Introduction to Network Simulator NS2. Springer, New York (2009)
24. Sajjad, S.M.: Neighbor node trust based intrusion detection system for WSN. In: 6th International Conference on Emerging Ubiquitous Systems and Pervasive Networks, EUSPN-2015 (2015)

Opinder Singh received his MCA degree from Guru Nanak Dev University, Amritsar, Punjab, India, in 2008. He has been in the teaching profession since 2008. He published 12 international research papers as well as 1 highly acclaimed textbook. Presently, he is research Scholar at Department of Computer Applications, IKG PTU, Kapurthala, Punjab, India. His research interests include Computer network, Adhoc network, and network security.

Jatinder Singh received his M. Tech degree from Punjabi University, Patiala in 2003 and Ph.D. degree from Punjabi University, Patiala, in 2011. He is a prolific author in the field of computer engineering. He has also won best research scholar award by UGC and management excellence award by MIDI, Punjab. He published 50 National and International research papers over the years as well as 20 highly acclaimed text and research books. He is also a member of several professional, scientific organizations and has lectured widely at academic institutions in India and Abroad.

Ravinder Singh received the B.Sc. Computer Science degree in 1996 and M.Sc. in 1998 from Guru Nanak Dev University, Amritsar, Punjab, India. He has received Ph. D. degree from Guru Nanak Dev University, Amritsar, Punjab, India in 2008. He has been in the teaching profession since 1999. Presently, he is working as Assistant Professor in the Department of Applied Sciences, Beant College of Engineering and Technology, Gurdaspur, Punjab, India. He published 21 international research papers.